| | |
|---|---|
| On Their Own Terms: A Lexicon with an Emphasis on Information-Related Terms Produced by the U.S. Federal Government<br><br>4th edition, revised<br>December, 2009<br><br>Susan L. Maret Ph.D. |  |

## Notes on the 4th edition

Since the first edition in 2005, *On Their on Terms* has reported language that reflects the scope of U.S. information policy. Now in its fourth edition, the *Lexicon* features new terms that further chronicle the federal narrative of information and its relationship to national security, intelligence operations, and freedom of information, privacy, technology, and surveillance as well as types of war, institutionalized secrecy, and censorship. This fourth edition also lists information terms of note that arise from popular culture and the scholarly literature.

This fourth edition of the *Lexicon* emphasizes the historical aspects of U.S. information policy and associated programs in that it is a testament to the information politics of the Bush-Cheney years; there is also a look back to historical agency recordkeeping practices such as the U.S. Army's *computerized personalities database*, serendipitously discovered in a 1972 congressional hearing on military surveillance of civilians[1] and the 1970s DoD program *Project Camelot*, which has parallels with *Project Minerva* efforts to recruit academics.[2] Including these

[1] Does CIFA (the Counterintelligence Field Activity) have roots in the Army's Counterintelligence Records Information System (CRIS), also called the Fort Monroe Data Bank? Or *Talon?* I leave it to FOIA researchers and historians to answer these questions; see *Army Surveillance of Civilians: A Documentary Analysis*, available at The Memory Hole, http://www.thememoryhole.org/2009/05/army-surveillance/ and *Uncle Sam is Watching You: Highlights from the Hearings of the Senate Subcommittee on Constitutional Rights* (Washington: Public Affairs Press, 1971).

[2] For additional discussion of the role of academia and the military and university as "hypermodern militarized knowledge factory," see John Armitage, "Beyond Hypermodern Militarized Knowledge Factories," *Review of Education, Pedagogy, and Cultural Studies* 27 (2005):219-239 and Henry A. Giroux's *The University in Chains: Confronting the Military-Industrial-Academic Complex* (Boulder, CO: Paradigm Publishers, 2007).

programs alongside contemporary federal information initiatives and public policy critiques furthers the "history of 'govermentality,' " an inquiry put forth by Michel Foucault (1994,1978: 219-222) that examines the "ensemble formed by the institutions, procedures, analyses, and reflections, the calculations and tactics that allow the exercise of this very specific albeit complex form of power." This latter thought suggests an active, genealogical role for FOIA researchers, archivists, historians, information professionals, and public interest groups in not only rescuing lost histories but integrating findings into existing understanding of federal information practices.

Throughout the *Lexicon*, links have been verified and replaced. However, in certain instances, Web pages and documents have been removed by the issuing federal agency. Considering the historical and archival importance of this information, links to the original source at the Wayback Machine is included.

## Introduction

*On Their Own Terms* is a lexicon of information-rich terms created by the U.S. legislative, regulatory, and policy process, and routinized by various branches of the U.S. government. These terms represent a virtual seed catalog to federal informationally-driven procedures, policies, and practices involving among other matters, the information life cycle, record keeping, ownership over information, collection and analysis of intelligence information, security classification categories and markings, censorship, citizen right-to-know, deception, propaganda, secrecy, technology, surveillance, threat, national security, and forms of warfare.

The abundance of federally produced information terms as reported in the *Lexicon* illustrates the sheer weight that rests on federal agencies in grappling with every aspect of information: communication, control, integrity, management, organization, preservation, production, and security. *Lexicon* terms also reflect the role federal agencies play in constructing a somewhat standardized, specialized language that orchestrates government policies and communicates national and international interests among fellow agencies, with Congress, the public, and the international community. In speaking of the specialized language of the Air Force Space Command (AFSPC) as an example, Lt. Col. Dana Flood (2008: 31) notes

> In the quarter-century of its existence, AFSPC has, like all large organizations, evolved over time to develop its own language, jargon, and terminology. Unfortunately, by

> accident, function, or design, AFSPC was largely a separate entity from the rest of the Air Force. Thus, like an isolated culture on a remote island, AFSPC's language developed to a point that it became a separate dialect, sometimes incomprehensible to the parent Air Force culture.

While language provides a group the means to identify within a given culture or political entity (Mueller 1973: 18), theorists such as David John Farmer (1995:1) claim that language is "more than a tool for thinking, for conceiving and communicating thoughts;" it is also a "factory of ideas, approaches, intuitions, assumptions, and urges" that mirrors and shapes the lifeworld. In addition to "sanctifying action" (Edelman 1964: 114), Jean-Jacques Lecercle (1999:47) observes that language is not a "simple representation" of the world, but an intervention within it. Lecercle writes that "words do not only do things, they are things."

In his "Glossary of Dispossession," writer Paul de Rooij observes "words are very important. Words frame issues, palliate, mollify, exculpate or even hide sordid acts." Many terms reported in the *Lexicon* meet de Rooij's description, representing a federal language of control that often downplays the significance of government actions, policies, and programs.[3] "Firstfruits," "National Censorship," "Public Diplomacy," and "Rendition," couch questionable policies and practices, and serve to legitimate authority, control over information, and public awareness of agency actions. Described by Claus Mueller (1973:24)[4] as "distortion" because "conditions and policies are quite different from their meanings," many *Lexicon* terms constitute a political language that "is designed to make lies sound truthful and murder

[3] Deborah Tannen (1998: 14) cites Dwight Bolinger's work in making the point that "language is like a loaded gun." Tannen observes the "terms in which we talk about something shape the way we think about it – even what we see."

[4] Mueller powerfully illustrates his concept of *distortion* by offering examples of "reformulated language," from the *Meyers Lexicon* published in the Weimar Republic in 1924, under National Socialist Germany in 1936, as Language Regulations issued by the Office of the Press (*Reichspressant*).

respectable and to give an appearance of solidity to pure wind" (Orwell 1950:92). Another way of viewing this is that "*language* often masks administrative evil" (Adams and Balfour 1998:15).[5]

## Information Terms as Bureaucratic Vocabulary: A Review

Robert P. Watson (1998:389) observes "despite the widespread use of bureaucratese, there has been insufficient research devoted to the study of the language of bureaucracy, and little is known about its effect." Srikant Sarangi and Stefan Slembrouck (1996:7) go further, questioning if the language of bureaucracy is a [*sic* specialized] language used in bureaucratic settings, or if is it language used in a particular way. In response to Watson, Sarangi and Slembrouck, I pose that *Lexicon* terms comprise a specialized, *evolving* language that is created and employed across bureaucratic[6] settings by federal agencies, which should really be thought of as "information societies."[7] With origins in law, regulation, territory, customary practices (relics or habits[8]), power, "hidden arrangements" (Sjoberg, Vaughn and Williams, 1984:446), and rational legal authority, these terms communicate and direct government policy across agencies, to the Congress, and the public. The terms listed in this work, which form the "language of bureaucracy," permeate every aspect of the federal information system. At times, this system affronts citizen and congressional understanding of federal information practices,

---

[5] For example, the Central Intelligence Agency's term "extraordinary rendition," is a term that masks the chilling dimensions of "outsourcing" torture and human rights violations.

[6] Bureaucracy as used in this work follows Max Weber's (1958: 196-198) description of "ideal" bureaucracy. That is, activity, authority, and the fulfillment of duties are distributed in a fixed way to constitute bureaucratic authority. This system is found in all bureaucratic structures as well as large party organizations and in management of the modern office, or bureau, which is based upon written documents ("the files").

[7] Definitions of information society include: spectacular technological innovation; involvement in knowledge production, new knowledge; reliance on those workers skilled in information handling and technology; spatial considerations wherein information networks, computer and communications technologies provide infrastructure for monitoring/governing; cultural acceptance and response to government information-saturated environments (for example, e-government, "digital governance," e-permitting, e-filing of taxes, etc.). Based in part on Webster (1995:6-23) and Weber, who Beniger (1986:6) believes was the first social scientist to see bureaucracy as a type of "critical new machinery."

[8] See Anthony Giddens (1994: 101).

and has serious consequences for what James Russell Wiggens has outlined as the right-to-know. [9]

A review of sociological, legal, and political science literature is helpful in positioning the problem of language in bureaucracy as a critical research problem:

■In general, the language of bureaucracy can be thought of as *technique*. Robert Merton (1964: vi) writes in the foreword to Jacques Ellul's *The Technological Society* that *technique* is "any complex of standardized means for attaining a predetermined result." With its contribution to precision, standardization of office practices and efficiency of transactions, especially related to information handling and information distribution, the information-laden language of federal information societies surely qualifies as *technique*.

- Max Weber's work in *Economy and Society*, which lends itself to the notion put forth in this work that language reflects the qualities of the office, or bureau, specifically the "technical superiority" of the bureaucracy as a form of human organization with goals of administrative precision, efficiency, and certainty. The two pillars of government, written laws and budget, require the merging of the files[10] by highly skilled bureaucrats who have the technical knowledge and skills to navigate the administrative landscape (Weber 1958: 196).

A look back to the 1972 Subcommittee on Constitutional Rights hearings on *Army Surveillance of Civilians: a Documentary Analysis* emphasizes the necessary role of the files in surveillance and control, mirroring what Harley (1988:279) characterizes as "all the retention and control of information and knowledge" :

> The core of any intelligence operations is its files. The Army's files on civilian political activity were voluminous and far reaching. Scores of local, regional, and national records centers kept track of individuals and organizations of all kinds, from the Unitarian Church, congregations to the Weathermen. Computers were used to store information

[9] Wiggens believes "the people's right to know is really a composite of several rights: It has at least five broad, discernible components: 1. the right to get information; 2. the right to print without prior restraint; 3. the right to print without fear of reprisal not under due process; 4. the right of access to facilities and material essential to communication; and 5. the right to distribute information without interference by government acting under law or by citizens acting in defiance of the law." *Freedom or Secrecy?* (New York: Oxford University Press, 1956). 3-4.

[10] For the purposes of this work, think information and its transmission occurring in all formats, incarnations and states, not only its physicality as represented in Weberian paperbound files.

> and to index voluminous libraries of dossiers. Where computers were not used, card indexes opened the way to information. (1972: 1)

Weber (1978: 255) writes that bureaucratic administration fundamentally means *domination through knowledge*, a feature that makes it specifically rational. Further, rationalization might be considered as the destruction or ignoring of information in order to facilitate its processing (Beniger 1986:15). Also at play is Giddens' (1987:178) idea that all states are information societies, but the nation-state has brought the gathering, storage and control of information to a "higher pitch" than at previous times in history. [11]

- Perrow, Reiss and Wilensky (1979:26) believe organizations develop a set of concepts influenced by a technical vocabulary, which include classification schemes that permit ease of communication within levels of the bureaucratic structure. Anything that does not fit into these "set" concepts, or procedural language, is not easily communicated.

- Claus Mueller (1973:14-15,18) theorizes that language acts as a "cultural and political guidance system into which values handed down from the past" that "enables" group identity, political stability, cohesion of values, and unification of interests. Extending Mueller's idea to *Lexicon,* it is posited that bureaucratic and agency specific language, along with conveying legal directive for action and policy, reflects the cultural heritage of federal agencies, such as member agencies of the Intelligence Community and Department of Defense.[12]

- In part, bureaucratic languages are based in rulemaking and the law. As Karl Olivecrona (1971: 254) writes, legal language is a "directive language" that is used for conveying information. I argue that directive (codified) language as reported in this work also acts to institutionalize specific categories of information, information-handling practices,[13] forms of censorship, information gathering, thus influencing information restriction and quality, including that of secreting and distorting information.

---

[11] The nation-state for Giddens (1987: 267) is characterized as "entities in the world system, in which a bipolar distribution of industrial and military power is pre-eminent." Giddens classifies nation-states into six categories; the United States (and the former USSR) is a "class one," "focal/hegemonic" entity that has a hegemonic position, which occupies a dominant position with the world. Power is "bipolar" in U.S. policy: it is a tension on the world stage between nuclear arms and a retreat into isolationism.

[12] See Jan Goldman's fascinating *Words of Intelligence: A Dictionary* [Scarecrow Press, 2006] and Rob Johnston's "disfavored" publication pulled from the CIA website in early 2006 *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*, [Washington, D.C., Central Intelligence Agency, 2005], online at FAS [of course!] http://www.fas.org/sgp/news/secrecy/2006/04/042806.html

[13] By "information handling practices," I include the mechanical aspects of information processing, preservation, access, life cycle, classification, and so on, as well as regulatory, and determinative language acts.

■In addition to conveying information about the administrative aspects of government, bureaucratic language also bestows authority over ownership of information to individual agencies, extending property rights over of information production, access, and dissemination of select types of information. The term *information owner, "*an official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal" (Committee for National Security Systems 2003), is one such term that supports the idea of information as agency property with intrinsic rights in controlling access to information.

Contrasting EO 13292 with the Office of Management and Budget's definition of information as "any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual," [14] creates dissonance that involves federally competing notions of public information.

■I also suggest the language of the bureaucracy is tied to the rise of *governmentality*, which Michel Foucault (1994:220-221) defines as a complex process occurring primarily in countries of the West that "transformed into the administrative state during the fifteenth and sixteenth centuries and gradually became 'governmentalized,' " into an "ensemble formed by the institutions, procedures, [*sic*, language and discourse] analyses, and reflections, [which include] the calculations and tactics that allow exercise of a very specific albeit complex form of power. "

Following Michel Foucault's work in discourse analysis, Dryzek (2005:9) writes that discourse is "a *shared way* of apprehending the world." Discourses are "embedded in language," and enable those who "subscribe to it interpret bits of information and put them into coherent stories or accounts." Discourses allow for the construction of "meaning, and relationships, and define legitimate knowledge," and rest on "assumptions, judgments, and contentions that provide the basic terms for analysis, debates, agreements and disagreements." The information-laden language of federal agencies qualifies as *discourse*.

■Reflecting Pierre Bourdieu's (1991:45) idea that language is bound to the state, and "imposes itself on the whole population as the only legitimate language," terms reported in the *Lexicon* direct and regulate the affairs of government and moderate understanding of policy.

■At it most elemental level, it can be conjectured the language of bureaucracy is *communicative action*, or "that form of social interaction in which the plans of action of different actors are coordinated through an exchange of communicative acts, that is, through a use of language orientated towards reaching understanding" (Habermas 1981:44).

---

[14] Circular No. A-130, "Management of Federal Information Resources." February 8, 1996, http://www.whitehouse.gov/omb/circulars/a130/a130.html

■ Postmodern (PM) expression permeates the federal information machine, most notably represented by the language created by the U.S. military and intelligence community (IC). For these entities, information acts

> "…as a weapon, as a myth, as a metaphor, as a force multiplier, as an edge, as a trope, as a factor, as an asset, information (and its handmaiden–computers to process it, multimedia to spread it, systems to represent it) has become the central sign of postmodernity." (Gray 1997:22) [15]

Postmodern federal language reflects the multifarious nature of information activities, including the rise of the "new global optics" of surveillance and spying (Virilio 2000:61). Information gathered from a labyrinthine amount of electronic devices and telecommunication sources is re-patterned from intelligence, surveillance, and forecasting tools into a type of Postmodern War, or *Wisdom Warfare.* [16] Provocative information terms such as the Department of the Army's *Information Fratricide* suggests a link to Orwell's *1984*; the U.S. Air Force *Modus Operandi Database* is reminiscent of Philip K. Dick's *Minority Report*'s analytical machinery "recording prophecies…carefully" listening.

## The Regulatory and Statutory Basis of Federal Language

Harold C. Relyea (2005:1-2) reports the Housekeeping Statute of 1789, codified in 1875, and also known as 5 U.S.C. 22, [17] authorized federal department heads to "prescribe regulations regarding custody, use, and preservation of records, papers, and the property of their entity." [18] U.S. laws such as the Administrative Procedure Act, the Atomic Energy Act of

---

[15] Postmodernity (PM) is a controversial notion; for example, Jean-Francois Lyotard's definition of PM as the "incredulity toward metanarratives" embodies the idea of the fusion of the self and personal life with "relations of time-space" (Giddens 1994: p. 59). We are caught up in "everyday experiments" whose outcomes are as open as those affecting humanity as a whole – these experiments should be seen as the "displacement and reappropriation of expertise under the impact of the intrusiveness" of abstract technological systems (Giddens 1994: 59-60).

[16] See David Lyons' various works, especially *Surveillance after September 11* (Polity; Malden, MA , 2003); Christopher Dandeker's *Surveillance, Power, and Modernity : Bureaucracy and Discipline from 1700 to the Present Day* (New York: St. Martin's Press, 1990); Jay Stanley and Barry Steinhardt's *Bigger Monster, Weaker Chains : the Growth of an American Surveillance Society*. (New York, NY : American Civil Liberties Union, 2003), http://www.aclu.org/Files/OpenFile.cfm?id=11572.

[17] Now codified as Title 5 > Part I > Chapter 3 > § 301.

[18] See *Amending Section 161 of the Revised Statutes with Respect to the Authority of Federal Officers and Agencies to Withhold Information and Limit the Availability of Records*. [85th Congress, 2d Session. H.R. Rep. No. 85-1461 to accompany H.R. 2767. (March 6, 1958). Serial Set no. 12072, "House Miscellaneous

1946 & 1954, the Antiterrorism and Effective Death Penalty Act of 1996, the National Security Act of 1947, the Classified Information Procedures Act, the Homeland Security Act of 2002,and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (US Patriot Act"), along with agency regulations, numerous Presidential Decisions Directives, Executive Orders (EO), most notably 8381, 10104, 12356, 12958,and 13292, Memoranda, and Freedom of Information Act exemptions enable agencies to carve out information policy and territory. This complex system of laws and regulations gives rise to specialized information categories, restrictions on information, information-handling practices, and information rules, some formalized, some not, that ultimately determine interagency,

---

Reports on Public Bills I"]. The housekeeping statute was "enacted to help General Washington get his administration underway by spelling out the authority for executive officials to set up offices and file government documents…the statute has been cited as authority to refuse information...but concealment has been the result of the application of 5 to an area where Congress has neglected to act over the years, while executive officials have let every file clerk become a censor" comments of Mr. Dawson (1-2). The report is compelling for its debate challenging an unequivocal right to know; see Clare E. Hoffman's (24) comments that total right to know would end any "confidential exchange of ideas." **Also see** *Availability of Information from Federal Departments and Agencies.* [Hearings before a subcommittee of the Committee on Government Operations, House of Representatives, Eighty-fourth Congress, first session-Eighty-fifth Congress, second session. Washington, D.C.: U.S. Government Printing Office, 1958; Y4.G7:IN3/], especially Parts 11 and 14 testimony on the Housekeeping Statute.

In addition, John J. Mitchell's (1958:200) research on the "custody, use, and preservation" language in the Housekeeping Act is interesting for its insight into the intent of the Act. Mitchell writes that various definitions are the same today as they were in 1789: "custody" denotes guarding or safekeeping; "use" involves application or employment; "preservation" implies protection from injury or destruction. These definitions do not justify any withholding or limiting of the availability of records. The substitution in the statute of any word or phrase from any of the above definitions cannot conceivably give rise to a right to withhold information or deny access to records. In fact, the definitions would imply availability of records, and that was the intent of Congress. Mitchell notes that although secrecy and claims of privilege have been the result of the Housekeeping Statute, "an exhaustive search of legislative history reveals no intent to provide for secrecy or the withholding of information." Mitchell argues "…the key words which have been so tortured are custody, use, and preservation." The definitions of these words are the same today as they were in 1789: "custody denotes guarding or safekeeping"; "use involves application or employment"; "preservation implies protection from injury or destruction. These definitions do not justify any withholding or limiting of the availability of records. The substitution in the statute of any word or phrase from any of the above definitions cannot conceivably give rise to a right to withhold information or deny access to records. In fact, the definitions would imply availability of records, and that was the intent of Congress."

public, and congressional access to information.

## The Secret Side of the Language [19]

As much as this *Lexicon* is an administrative-regulatory dictionary of information terms, it is also a guide to the language of secrecy in that it pays homage to Daniel Patrick Moynihan's (1997) thought that two [information] "regimes" exist today in the United States. The first regime according to Moynihan, is public regulation for disclosure, discovery, and due process, and is under constant scrutiny. The second regime is "concealed within a vast bureaucratic complex," wherein "some congressional oversight may take place and some Presidential control." In this latter regime, the public is not excluded altogether, but the system is fraught with secrecy and "misadventure."[20] Secrecy, as supported by the multitudinous classifications, designations, and markings as listed in the *Lexicon* attest to the complexity of the U.S. secrecy system and the language that enables its authority and power over information. The language of secrecy can be thought of as a form of *jargon*, where information is "replaced with *classified*, which makes things less conspiratorial and at the same time creates visions of busy, efficient people classifying documents in a scientific way" (Bolinger 1980: 132).

Moreover, ambiguous information security markings, or "pseudo-classifications," many defined here in the *Lexicon*, practically serve as *de facto* firewalls preventing information access and creating information asymmetries from agency to agency, Congress, and citizens. It has been suggested that pseudo-classifications also have "persistent and pernicious" effects on the flow of threat information.[21] In its *2004 Report to the President*, the Information Security Oversight Office wrote:

---

[19] For a deep review of government secrecy, see Maret and Goldman, *Government Secrecy: Classic and Contemporary Readings.* Libraries Unlimited, 2008.

[20] From the *Congressional Record* May 1, 1997.

[21] Rep. Christopher Shays. "Emerging Threats: Overclassification and Pseudo-Classification." Hearing before the Subcommittee on National Security, Emerging Threats, and International Relations Committee

> Limitations on dissemination of information that are designed to deny information to the enemy on the battlefield can increase the risk that our own forces will be unaware of important information, contributing to the potential for friendly fire incidents or other failures.
>
> Likewise, imposing strict compartmentalization of information obtained from human agents increases the risk that a Government official with access to other information that could cast doubt on the reliability of the agent would not know of the use of that agent's information elsewhere in the Government.
>
> The National Commission on Terrorist Attacks Upon the United States noted that while it could not state for certain that the sharing of information would have succeeded in disrupting the 9/11 plot, it could state that the failure to share information contributed to the government's failure to interrupt the plot. Simply put, secrecy comes at a price.[22]

### Organization of this Work

For most entries, terms are direct quotes from U.S. government agency-produced unclassified open sources and declassified information available in print and on the Web. Among other federal publications, the *Federal Register*, *Code of Federal Regulations*, and the *U.S. Code* were consulted in order to provide additional views of codified interpretations of information language and information-related activities. For government publications sources available exclusively in print, the SuDoc (Superintendent of Documents) call number is included, wherein documents in print and microfiche format can be located in government publications sections of most libraries.[23] I deliberately employed an "in their own words" format to demonstrate language at work. In addition to these elements, multiple agency interpretations

---

on Government Reform. House of Representatives 109th Congress, First Session, March 2, 2005, http://www.fas.org/sgp/congress/2005/030205overclass.html

[22] Information Security Oversight Office. *2004 Report to the President*, .http://www.archives.gov/isoo/reports/2004-annual-report.html

[23] Federal Web pages, Web sites, and documents come and go. This ephemeral condition of imformation presents a challenge in compiling the *Lexicon*. I remain grateful to the Federation of American Scientists (FAS), National Security Archive (NSA), OMB Watch, EPIC, EFF, and the many public interest groups that preserve critical historical documents, and hence the public right to know.

and definitions are provided to illustrate how agencies have interpreted, often widely, the same Executive Orders, public laws, regulations, memoranda, and internal directives in devising their own agency-specific information language. This scenario holds most true in the case of information security-related terms. As the Joint Security Commission (1994) reports,

> US Government security policies and practices have evolved in an ad hoc manner over the last four decades. Security policy is enunciated in a collection of documents (Executive Orders, National Security Decision Directives, National Security Directives, Presidential Decision Directives, legislation, and individual department or agency directives and orders) prepared at different times, by different people, in response to different requirements and events, not as part of a coherent planned effort.

Every effort was made to verify and accurately report origins and sources of terms. In verifying terms, especially the Byzantine terms arising from the intelligence community, I hope I have cleared up significant problems I see with accurate interpretation, historical context, and citation of sources often lacking in popular works and on Websites. Lastly, mirroring Gilles Deleuze's observation that "a concept sometimes needs a new word to express it, sometimes it uses an everyday word that gives it a singular sense," included are terms from my research that I hope further elucidates information categories and concepts not well represented in the scholarly literature.[24]

Practically speaking, the *Lexicon* is intended for use by citizens, students, and researchers who struggle to understand the complex language of the federal information machine. The *Lexicon* is also geared to those individuals who, in using the Freedom of Information Act (FOIA) to request government information, may be unfamiliar with specific history or terms related to files, records, and the more occult areas of security classification and markings.[25]

---

[24] Such as *nuclear secrecy*, this work.

[25] Obviously this guide is not designed for certain members of the IC, who have a very different understanding of the procedural and legal aspects of handling classified, and potentially sensitive information, and may find certain aspects of this work naïve or simplistic. This work is for the rest of us.

To this end, Ludwig Wittgenstein (1958:199) writes that to "understand a language means to be master of a technique." It is my hope the *Lexicon* contributes to further understanding of the role of language and it's influence on access to government information, encouraging citizens and researchers alike to look beyond the often emblematic language of bureaucracy to the essence of words and actions, and their relationship with direct democracy.

### Works Cited


Adams, Guy B., and Danny L. Balfour. *Unmasking Administrative Evil.* Thousand Oaks, CA: Sage Publications, 1998.

Beniger, James R. *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge, MA: Harvard University Press, 1986.

Billig, Michael. "Critical discourse analysis and the rhetoric of critique." Ed. Gilbert Weiss and Ruth Wodak. *Critical Discourse Analysis: Theory and Interdisciplinarity.* New York: Palgrave Macmillan, 2003. 35-46.

Bolinger, Dwight. *Language, the Loaded Weapon.* New York: Longman Group, 1980.

Bourdieu, Pierre. *Language and Symbolic Power*. Ed. John B. Thompson. Trans. Gino Raymond and Matthew Adamson. Cambridge, MA: Harvard University Press, 1991.

Dick, Philip K. *The Minority Report*. New York, NY: Carol Publishing Group, 1991.

De Rooj, Paul. "A Glossary of Dispossession." *Dissident Voice* (2 January 2006). 1 June 2009 <http://www.dissidentvoice.org>.

Dryzek, John S. *The Politics of the Earth: Environmental Discourses*. New York: Oxford University Press, 2005.

Edwards, Paul N. *The Closed World: Computers and the Politics of Discourse in Cold War America.* Cambridge: MIT Press, 1996.

Edelman, Murray J. *The Symbolic Uses of Politics*. Urbana: University of Illinois Press, 1967.

Ellul, Jacques. *The Technological Society*. Trans. John Wilkinson. New York: Alfred Knopf, 1964.

Farmer, David John. *The Language of Public Administration : Bureaucracy, Modernity, and Postmodernity.* Tuscaloosa: University of Alabama Press, 1995.

Foucault, Michel. *Discipline and Punish*: The Birth of the Prison. Trans. Alan Sheridan, New York: Vintage Books, 1995.

_____. "Governmentality." *Power*: *The Essential Works of Foucault 1954-1984*. Volume 3. Ed. James D. Faubion. Trans. Robert Hurley. New York: The New Press, 1994.

_____. *Language, Counter-Memory and Practice: Selected Essays and Interviews.* Ed. Donald F. Bouchard. Trans. Donald Bouchard & Sherry Simon. New York: Cornell University Press, 1977.

_____. "Order of Discourse." *Social Science Information* 10 no. 2 (1971): 7-30.

_____. *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977.* Ed. and Trans. Colin Gordon. New York: Pantheon Books, 1980.

Flood, Dana. "Common language, common culture: how the space community must change language and perspective to achieve cross-domain integration and dominance*." High Frontier* 4 no. 4 (August 2008): 31-34. 1 June 2009 <http://www.afspc.af.mil/shared/media/document/AFD-080826-020.pdf>.

Giddens, Anthony. (1994). "Living in a post-traditional society." Ed. Ulrich Beck, Anthony Giddens and Scott Lash. *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order*. Stanford: Stanford University Press. 56-109.

_____. *The Nation-State and Violence*. Berkeley: University of California Press. 1987.

_____. *Politics and Sociology in the Thought of Max Weber*. London, Macmillan, 1972.

Gray, Chris Hables. "Perpetual revolution in military affairs, international security, and information. " Ed. Robert Latham. *Bombs and Bandwidth: the Emerging Relationship between Information Technology and Security*. New York: New Press, 2003. 199-214.

_____. *Postmodern War: The New Politics of Conflict*. New York: Guilford Press, 1997.

Habermas, Jurgen. *The Theory of Communicative Action*. Trans. Thomas McCarthy. Boston: Beacon Press, 1984-1987.

Harley, J.B. "Maps, knowledge and power." Ed. Denis Cosgrove & Stephen Daniels. *The Iconography of Landscape: Essays on the Symbolic Representation, Design, and Use of Past Environments.* New York: Cambridge University Press, 1988. 277-311.

Joint Security Commission. "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence." 28 February 1994. Federation of American Scientists Web site. 1 June 2009 <http://www.fas.org/sgp/library/jsc/>.

Lakoff, George, and Mark Johnson. *Metaphors We Live By*. Chicago: University of Chicago Press, 1980.

Lecercle, Jean-Jacques. *The Violence of Language.* New York: Routledge, 1990.

Lutz, William. *Doublespeak.* New York: Harper & Row, 1989.

_____. *The New Doublespeak: Why No One Knows What Anyone's Saying Anymore*. New York: HarperCollins, 1996.

Lyotard, Jean-Francois. *The Postmodern Condition: A Report on Knowledge*. Trans. Geoff Bennington and Brian Massumi. Minneapolis: University of Minnesota Press, 1984.

Mills, C. Wright. "Language,logic and culture." Ed. Irving Louis Horowitz. *Power, Politics and People*: *The Collected Essays of C. Wright Mills.* New York: Oxford University Press, 1963. 423-438.

_____. *The Power Elite*. New York: Oxford University Press, 1956.

Mitchell, John J. "Government Secrecy in Theory and Practice: 'Rules and Regulations' as an Autonomous Screen." *Columbia Law Review* 58 no. 2 (1958): 199-210.

Moynihan, Daniel. "Secrecy as Government Regulation." *Congressional Record* 1 May 1997. Federation of American Scientists Web site. 1 June 2009 <http://www.fas.org/irp/congress/1997_cr/h970501-moynihan.htm>.

Mueller, Claus. *The Politics of Communication.* New York, Oxford University Press, 1973.

Olivecrona, Karl. *Law as Fact*. London: Stevens, 1971.

Orwell, George. "Politics and the English language." *Shooting an Elephant*. New York: Harcourt Brace, 1950. 77-92.

Perrow, Charles, Albert Reiss, Jr., and Harold L. Wilensky. *Complex Organizations: A Critical Essay.* 3rd ed. New York: McGraw-Hill, 1986.

Rabinow, Paul. (Ed.). *Essential Works of Michel Foucault, 1954-1984.* New York: New Press, 2000.

Relyea, Harold. "Access to Government Information in the United States." *CRS Report to Congress* 7 January 2005. Federation of American Scientists Web site. 1 June 2009 <http://www.fas.org/sgp/crs/97-71.pdf>.

Sarangi, Srikant, and Stefaan Slembrouck. *Language, Bureaucracy, and Social Control*. Longman: New York, 1996.

Sjoberg, Gideon, Ted R. Vaughan, and Norma Williams. Bureaucracy as Moral Issue. *Journal of Applied Behavioral Science* 20 no. 4 (1984): 441-453.

Tannen, Deborah. *The Argument Culture: Moving from Debate to Dialogue.* New York: Random House, 1998.

United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Army Surveillance of Civilians: A Documentary Analysis*. 92nd Congress, second session. Washington, D.C.: U.S. Government Printing Office, 1972. The Memory Hole. 1 June 2009 <http://www.thememoryhole.org/2009/05/army-surveillance/>.

Virilio, Paul. *The Information Bomb*. Trans. Chris Turner. New York: Verso, 2000.

Watson, Robert D. "On the language of bureaucracy: postmodernism, plain English, and Wittgenstein." Ed. Thomas D. Lynch & Todd J. Dicker. *Handbook of Organization Theory and Management: the Philosophical Approach.* New York: M. Dekker, 1998. 389-413.

Weber, Max. *Economy and Society: An Outline of Interpretive Sociology*. Trans. Ephraim Fischoff. Ed. Guenther Roth and Claus Wittich. Berkeley: University of California Press, 1978.

_____. *From Max Weber: Essays in Sociology*. Ed. and trans. H. H. Gerth and C. Wright Mills. New York: Oxford University Press, 1958.

Webster, Frank. *Theories of the Information Society*. New York: Routledge, 1995.

Wiggins, James Russell. *Freedom or Secrecy?* New York: Oxford University Press, 1956.

Wittgenstein, Ludwig. *Philosophical Investigations.* Trans. G.E.M. Anscombe. New York: Macmillan, 1958.

Woolard, Kathryn A. "Language ideology as a field of inquiry." Ed. Bambi B. Schieffelin, Kathryn A . Woolard, and Paul V. Kroskrity. *Language Ideologies: Practice and Theory*. New York: Oxford University Press, 1998. 3-47.

Yates, Joanne. *Control through Communication: The Rise of System in American Management.* Baltimore: Johns Hopkins University Press, 1989.

## Creative Commons License



## How to Cite This Work

Maret, Susan L. *On Their Own Terms: A Lexicon with an Emphasis on Information-Related Terms Produced by the U.S. Federal Government*. 4th edition, revised December, 2009, http://www.fas.org/sgp/library/maret.pdf

## Contact

You can drop me a line at: iecologie@yahoo.com

Thanks to all the folks who volunteered terms and offered advice on formatting.

## TERMS

---

**100 Percent Shred Policy**
Every Airman, civilian and contractor on base is responsible for destroying paper they create or use in their workspaces when they no longer need it.

The 100 percent shred policy requires a 3/8 inch crosscut shredder or better. People who do not have a shredder in their work center should work with their unit's OPSEC coordinator and resource advisor to find or procure one…

Source: USAF, Malstrom Air Force Base, "Getting into the habit: 100 percent shred policy begins March 17," http://www.malmstrom.af.mil/news/story.asp?id=123139099

**201 File**
The CIA opens a 201 file on an individual when it has an "operational interest" in that person. (p.45)

Source: Assassination Review Board, *Final Report of the Assassination Records Review Board*, September 1998, http://www.archives.gov/research/jfk/review-board/report/

---

**~ A ~**

**Able Danger**

***See Data Mining, Social Network Analysis***

In summer 2005, news reports began to appear regarding a data mining initiative that had been carried out by the U.S. Army's Land Information Warfare Agency (LIWA) in 1999-2000. The initiative, referred to as Able Danger, had reportedly been requested by the U.S. Special Operations Command (SOCOM) as part of larger effort to develop a plan to combat transnational terrorism. Because the details of Able Danger remain classified, little is known about the program. However, in a briefing to reporters, the Department of Defense characterized Able Danger as a demonstration project to test analytical methods and technology on very large amounts of data. The project involved using link analysis to identify underlying connections and associations between individuals who otherwise appear to have no outward connection with one another. The link analysis used both classified and open source data, totaling a reported 2.5 terabytes. All of this data, which included information on U.S. persons, was reportedly deleted in April 2000 due to U.S. Army regulations requiring information on U.S. persons be destroyed after a project ends or becomes inactive.

Source: Jeffrey W. Seifert. "Data Mining and Homeland Security: An Overview." *CRS Report to Congress* January 27, 2006. FAS Website, http://www.fas.org/sgp/crs/secrecy/RS20748.pdf.

2. For a background and history of the Able Danger program, see the IG report listed below. Figures 1-3, pages 8-9 have a very interesting social network analysis chart of alleged A-Qaeda cell links.

Source: DoD Office of the Inspector General (IG). "Report of Investigation." September 18, 2006. FAS Website,http://www.fas.org/irp/agency/dod/ig-abledanger.pdf and Rep. Curt Weldon. "Weldon Rejects DoD Report on Able Danger and Harassment of Military Office." http://www.fas.org/irp/news/2006/09/weldon092106.html

**Access**

1. The ability and means necessary to store data in, to retrieve data from, to communicate with, or to make use of any resource of a system; 2. To obtain the use of a resource; 3. capability and opportunity to gain detailed knowledge of or to alter information or material; 4. capability and means to communicate with (i.e., input to or receive output from), or otherwise make use of any information, resource, or component in an AIS. Note [for 3 and 4]: An individual does not have "access" if the proper authority or a physical, technical, or procedural measure prevents him/her from obtaining knowledge or having an opportunity to alter information, material, resources, or components, and 5. An assigned portion of system resources for one data stream of user communications or signaling.

Source: "Federal Standards Telecommunications"
http://www.its.bldrdoc.gov/fs-1037/dir-001/_0104.htm

2. The ability or opportunity to gain knowledge of classified information.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended.
http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2

**Access to Classified Information**
The ability and opportunity to obtain knowledge of classified information. Persons have access to classified information if they are permitted to gain knowledge of the information or if they are in a place where they would be expected to gain such knowledge. Persons do not have access to classified information by being in a place where classified information is kept if security measures prevent them form gaining knowledge of the information.

Source: Department of Defense. *DoD Dictionary of Military and Associated Terms.* JP 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**Accountability**
(IS) Process of tracing IS activities to a responsible source;(COMSEC, or Communications Security) Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*. June, 2006. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Accountability Information**
A set of records, often referred to as an audit trail, that collectively provides documentary evidence of the processing or other actions related to the security of an Automated Information System.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995,
http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

**Acknowledged Special Access Program (SAP)**
*See Special Access Program*

An existing SAP whose overall purpose is identified and its specific details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and risk of compromise.

Source: DoD Directive 5205.7 "Special Access Program (SAP) Policy." January 5, 2006, http://www.dtic.mil/whs/directives/corres/html/520507.htm

**Actionable Medical Information Review**

***See Prepublication Review***

Since 2006 U.S. Army censors have scrutinized hundreds of medical studies, scientific posters, abstracts and Powerpoint presentations authored by doctors and scientists at Walter Reed and other Army medical research centers—part of a little- known prepublication review process called "Actionable Medical Information Review." The program is intended to deny Iraqi and Afghan insurgents sensitive data such as combat injury and death rates. But dozens of studies reviewed under the program did not involve research directly related to combat operations. Instead, they described controversial topics like the effects of war on soldiers' children, hospital-acquired infections, post-deployment adjustment issues, refugees, suicide, alcoholism, vaccines, cancer among veterans and problems with military health care databases.

Source: EPI Medical News and Expose, "U.S. Army delays, alters medical studies under a little-known scientific censorship program," http://www.epinews.com/AMI.html

**Advanced Research Development Activity (ARDA)**

***See Disruptive Technology Office, In-Q-TEL***

1. ARDA's mission is to sponsor high-risk high-payoff research designed to leverage leading edge technology in the solution of some of the most critical poblems facing the intelligence community (IC). As such, ARDA's purpose is to incubate revolutionary research for the shared benefit of the intelligence community (IC) by originating and managing R&D Programs that :

- Have the potential to fundamentally impact future operational needs and strategies;
- Demand substantial, long-term, venture investment to spur risk-taking;
- Progress measurably toward mid-term and final goals; and
- Take many forms and employ many delivery vehicles.

Note: Superseded by the National Security Agency's Disruptive Technology Office.

Source: ARDA. Website previously available at http://www.ic-arda.org/ now through Wayback Machine http://web.archive.org/web/*/http://www.ic-arda.org/ [NOTE: typo left in.]

2. ARDA is an intelligence community (IC) organization whose mission is described as "to sponsor high-risk, high-payoff research designed to leverage leading edge technology to solve some of the most critical problems facing the Intelligence Community (IC)." ARDA's research support is organized into various technology "thrusts" representing the most critical areas of development. Some of ARDA's current research thrusts include Information Exploitation, Quantum Information Science, Global Infosystems Access, Novel Intelligence from Massive Data, and Advanced Information Assurance.

Jeffrey W. Seifert. "Data Mining: An Overview." *CRS Report for Congress* January 27, 2006, http://www.fas.org/sgp/crs/secrecy/RS20748.pdf

**Adverse Information**

***See Derogatory Information***

1. Any factual and verifiable unfavorable information that creates a question as to an individual's eligibility for access authorization or an entity's eligibility for a favorable Foreign Ownership, Control, or Influence determination (see "Derogatory Information," section 710.8 of Title 10, Code of Federal Regulations, below).

2. Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

Source: *National Industrial Security Program Operating Manual* (NISPOM). DoD 5220.22-M. January 1995, http://www.dtic.mil/whs/directives/corres/html/522022m.htm

3. Any information that adversely reflects on the ethics and compliance program of a company with a cleared facility, that suggests that the company's ability to safeguard classified information and/or special nuclear material may be impaired.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/nnglossary/termsa_j.pdf

**ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement)**

The term "ADVISE" has been used interchangeably for two different stages of research and development:

- The first refers to a toolset or development kit - a set of generic tools to gather, link, and present information.

- The second refers to a collection of deployed systems to test the effectiveness of the toolset in specific settings.

Since each of these references to "ADVISE" raises a different set of privacy protection risks, it is important to distinguish between the risks presented by a development kit and the risks presented by a deployed system. This report uses the following separate terms:

Source: DHS Privacy Office Review of the Analysis, Dissemination, Visualization, Insight and Semantic Enhancement (ADVISE) Program, July 11, 2007, http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_advise.pdf and CNet, "Report: DHS Kills Data-Mining Project," http://news.com.com/8301-10784_3-9773243-7.html

**Advisory Committee on Historical Diplomatic Documentation**

***See the Foreign Relations of the United States (FRUS)***

1. Established by PL102-138, the Foreign Relations Authorization Act, Fiscal Years 1992 and 1993, signed by President Bush on October 28, 1991. Section 198 of P.L. 102-138 added a new Title IV to the Department of State's Basic Authorities Act of 1956 (22 *U.S.C.* 4351, et seq.). The statute sets the membership of the Committee at nine members drawn from among historians, political scientists, archivists, international lawyers, and other social scientists who are distinguished in the field of U.S. foreign relations.

Six members represent the American Historical Association, the Organization of American Historians, the American Political Science Association, the Society of American Archivists, the American Society of International Law, and the Society of Historians of American Foreign Relations; there are also three "at large" members. The members are granted all necessary security clearances. The legislation requires that the Committee meet four times a year. The Historian of the State Department serves as executive secretary of the Committee. The Advisory Committee reviews records, advises, and makes recommendations to the Office of the Historian, Bureau of Public Affairs, concerning the Foreign Relations of the United States documentary series. The Committee monitors the overall compilation and editorial process of the series and advises on all aspects of the preparation and declassification of the series. Although the Committee does not review the contents of individual volumes, it does monitor the overall process and makes recommendations on particular problems that are brought to its attention. The Committee also reviews the declassification procedures of the Department of State, all guidelines used in the declassification process, and, by random sampling, documents representative of all Department of State records that remain classified after 30 years. The Committee is required to submit an annual report to the Secretary of State setting forth its findings from this review.

Source: Department of State. "Historical Advisory Committee." http://www.state.gov/r/pa/ho/aD.C.om/

and *Foreign Affairs Manual*. 10 FAM 141.2-2, "Foreign Relations of the United States." http://foia.state.gov/REGS/fams.asp?level=2&id=11&fam=0 and Office of the Inspector General, Management Review of the Office of the Historian Bureau of Public Affairs, U.S. Department of State, May 2009, http://oig.state.gov/documents/organization/124568.pdf

2. SEC. 403. PROCEDURES FOR IDENTIFYING RECORDS FOR THE FRUS SERIES; DECLASSIFICATION, REVISIONS, AND SUMMARIES.
`(1) to coordinate with the State Department's Office of the Historian in selecting records for possible inclusion in the FRUS series;
`(2) to permit full access to the original, unrevised records by such individuals holding appropriate security clearances as have been designated by the Historian as liaison to that department, agency, or entity, for purposes of this title, and by members of the Advisory Committee; and
`(3) to permit access to specific types of records not selected for inclusion in the FRUS series by the individuals identified in paragraph (2) when requested by the Historian in order to confirm that records selected by that department, agency, or entity accurately represent the policymaking process reflected in the relevant part of the FRUS series.

Source: PL102-138, the Foreign Relations Authorization Act.,
http://ftp.fas.org/sgp/advisory/state/pl102138.html

**Advisory Sensitivity Attributes**
User-supplied indicators of file sensitivity that alert other users to the sensitivity of a file so that they may handle it appropriate to its defined sensitivity. Advisory sensitivity attributes are not used by the AIS to enforce file access controls in an automated manner.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090 "Definitions of Diplomatic Security Terms." November 13, 2003. http://foia.state.gov/REGS/Search.asp

**Agency**
In intelligence usage, an organization or individual engaged in collecting and/or processing information

Source: Department of Defense. *DoD Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**Agencywide Documents Access and Management System (ADAMS)**
An information system that provides access to all image and text documents that the NRC has made public since November 1, 1999, as well as bibliographic records (some with abstracts and full text) that the NRC made public before November 1999.

Source: Nuclear Regulatory Commission (NRC).http://www.nrc.gov/reading-rm/adams.html

**Agility**

***See Power to the Edge***

Agility is related to the ability to conduct network-centric operations (NCO) and is associated with Power to the Edge principles. A robustly networked force is, by virtue of its increased connectedness, more agile. An improved information position clearly enables agility, while the concept of speed of command that is associated with a network-centric force is closely related to the responsiveness attribute of agility.

Source: Simon Reay Atkinson and James Moffat *The Agile Organization: From Informal Networks to Complex Effects and Agility*, DoD, CCRP, 2005, http://www.dodccrp.org/files/Atkinson_Agile.pdf

**Agnotology**

Attributed to linguist Ian Boa, the study of ignorance from *agnoia*, "want of perception or knowledge" and *agnosia*, "a state of ignorance or not knowing, both from gnosis meaning knowledge."

Source: Robert N. Proctor, "Agnotologuy: A Missing Term," *Agnotology: The Making and Unmasking of Ignorance* Robert N. Proctor and Londa Schiebinger, eds. Stanford Press: 2008. 27.

**Agreement on Trade-related Aspects of Intellectual of Property Rights (TRIPS)**

A WTO agreement that obligates countries to provide minimum standards of intellectual property (IP) protection in national laws and to enforce minimum standards for protecting intellectual property. The TRIPS Agreement covers copyright and related rights (that is, the rights of performers, producers of sound recordings, and broadcasting organizations); trademarks including service marks; geographical indications including appellations of origin; industrial designs; patents including the protection of new varieties of plants; the layout-designs of integrated circuits; and undisclosed information, including trade secrets and test data.

Source: Merritt R. Blakeslee and Carlos A. Garcia, *The Language of Trade* 3rd edition, 2001 Department of State, International Information Programs, http://www.4uth.gov.ua/usa/english/trade/language/index.htm

**Agricultural Chemical Usage Reports**

***See Right to Know***

Published by the Environmental, Economics, and Demographics Branch, United States Department of Agriculture, National Agricultural Statistics Service (USDA-NASS), the series reported pesticide usage on vegetables, postharvest, on farm animals, floriculture, and other applications. Issued through the federal depository system to libraries since 1990 and later online, the reports are the only publicly available data source on pesticide use in the U.S. and a valuable resource for farmers, the public, and policymakers in tracking pesticide usage and compliance with international bans on certain pesticides.

On May 21, 2008, USDA announced it is eliminating the program as it can no longer afford the program.

Source: OMB Watch, "USDA Dropping Shroud over Pesticide Use Data," http://www.ombwatch.org/node/3700 and GreenBiz.com, "USDA Cuts Pesticide-Use Data Reports," http://www.greenbiz.com/news/2008/05/28/usda-cuts-pesticide-use-data-reports

### All-Source Intelligence

1. Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence.

2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. (Army) – Intelligence that is produced through the analysis of all available information obtained through intelligence, surveillance, and reconnaissance (ISR) operations.

Source: Department of the Army. FM 2-0. Intelligence. May 2004, http:// www.fas.org/irp/doddir/army/fm2-0.pdf and Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

### Alternative Information Leakage

Steve: And that technology exists pretty well. Now, well, what's interesting is this is another in a long series of security and information leakage which is a function of electrical or mechanical or electromagnetic leakage from a computer. You know, we've all heard, you know, years ago there was this technology called Tempest, which was - it attempted to, and apparently successfully, determined what image you had on your screen based on the electromagnetic leakage from a CRT.

Leo: "Van Eck freaking" they call that, yeah.

Source: Leo Laporte, This is Security Now! Episode 6 for September 22, 2005, Steve Gibson, http://media.GRC.com/sn/SN-006.mp3

**Alternative Media** (U//FOUO)
A term used to describe various information sources that provide a forum for interpretations of events and issues that differ radically from those presented in mass media products and outlets.

Source: DHS, *Domestic Extremism Lexicon* Reference Aid March 26, 2009, http://www.scribd.com/doc/14884903/Domestic-Extremism-Lexicon-US-Department-of-Homeland-Security-Reference-Aid

**Alternative or Compensatory Control Measures**
***See Need-to-Know, Special Access Programs***
Department of Defense also uses the marking Alternative or Compensatory Control Measures (ACCM) for classified information that requires special security measures to safeguard classified intelligence or operations and support information when normal measures are insufficient to achieve strict need-to-know controls and where special access program (SAP) controls are not required. ACCM measures are defined as the maintenance of lists of personnel to whom the specific classified information has been or may be provided together with the use of an unclassified nickname. The ACCM designation is used in conjunction with the security classification to identify the portion, page, and document containing ACCM information.

Source: Defense Security Service. "Classification Guidelines And Distribution Controls Original and Derivative Classification." http://www.dss.mil/training/csg/security/S1class/Classif.htm; Head to Wayback Machine to view the doc, http://web.archive.org/web/20070317052725/http://www.dss.mil/training/csg/security/S1class/Classif.htm

**Altivore**
***See DCSNET***
1. [The] source code to "Altivore," a program that mimics all the capabilities of Carnivore. Part protest against Carnivore's potential for invasions of privacy and part defensive measure aimed at subverting Carnivore, Altivore is the latest escalation of the ongoing battle over just how much privacy we can expect in cyberspace.

Also, to give ISPs [Internet service providers] an alternative to the FBI. The FBI comes up with a search warrant and really, what the FBI wants, is just the data. They don't care how you get it. If

the ISP can use Altivore instead, they don't need to have this secretive black box on the network.

Source: Sean Dugan. "Defanging Carnivore." (interview with Altivore codewriter Robert Graham) *Salon* September 25, 2000, http://archive.salon.com/tech/view/2000/09/25/robert_graham/index.html

2. Dubbed "Altivore," the source code conforms to the features of Carnivore as described in the FBI's recent solicitation for independent review of its program. According to Network ICE, the FBI had requested that any university that wanted to review the software verify that it:

monitors suspect's e-mail (either headers or full content),
monitors suspect's access to certain types of servers, including Web and FTP servers,
copies all packets to and from the suspect's IP address, and
discovers the suspect's Internet address (when assigned by the ISP) by communicating with the provider's infrastructure.

Source: Robert Lemos. "Open-source Carnivore clone released." September 20, 2000, http://news.zdnet.com/2100-9595_22-524062.html

**Analysis and Production**
In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements.

Source: Department of Defense *DoD Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**Analyst Notebook I2**
***See Data Mining***
Information Analysis and Infrastructure Protection Directorate. Correlates events and people to specific information;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: Yes;
Features: Other agency data: No.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004. http://www.gao.gov/htext/d04548.html

**Anomaly**

An indication of foreign power activity or knowledge, inconsistent with the expected norm, that suggests knowledge of U.S. national security information, processes, capabilities, or activities. Reports of anomalies shall be made through appropriately secure channels.

Source: United States. Department of Justice. Justice Management Division. Information Security Policy Group. Classified national security information. Washington, D.C.: U.S. Dept. of Justice, Justice Management Division, Security and Emergency Planning Staff: Information Security Policy Group, 1998. SUDOC: J1.2:SE2/5

**Application**

In the intelligence context, the direct extraction and tailoring of information from an existing foundation of intelligence and near time reporting. It is focused on and meets specific, narrow requirements, normally on demand.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Archiving (Records)**

The maintenance of records in remote storage after a case has been closed or disposed of, as a matter of contingency, should the records be needed for later reference.

Source: DOJ, Global Justice Information Sharing Initiative, *Criminal Intelligence Glossary of Terms*, *Minimum Criminal Intelligence Training Standards*, Appendix, October 2007, http://www.it.ojp.gov/documents/min_crim_intel_stand.pdf

**Armed Forces Censorship**

***See Censorship***

The examination and control of personal communications to or from persons in the Armed Forces of the United States and persons accompanying or serving with the Armed Forces of the United States.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Assassination Record**

***See Record***

1. Section 1400.1 of the [*sic*, Assassination Review] Board's final definition of "assassination record" reads: (a) An assassination record includes, but is not limited to, all

records, public and private, regardless of how labeled or identified, that document, describe, report on, analyze, or interpret activities, persons, or events reasonably related to the assassination of President John F. Kennedy and investigations of or inquiries into the assassination (p.18).

2. The Review Board often turned back to the breadth of its definition of the term "assassination record told the Review Board that he did not believe that his office's records were assassination records because the records did not mention the assassination, or any of the central assassination figures. When it was defining the term "assassination record," the Board anticipated that federal agencies and others who possessed relevant records would challenge the Board's judgment (p.19).

Source: Assassination Review Board, *Final Report of the Assassination Records Review Board*, September 1998, http://www.archives.gov/research/jfk/review-board/report/

**Asymmetric| Asymmetric Information | Asymmetries of Information**
***See Deception, Information Dominance, Information Superiority, Information Warfare***

1. A byproduct of the information revolution that allows smaller players to compete as larger ones once did or do.

Source: David J. Rothkopf. "Cyberpolitik: The Information Revolution and U.S. Foreign Policy." March 22, 2000, http://www.carnegieendowment.org/events/index.cfm?fa=eventDetail&id=51

2. Dissimilarities in organization, equipment, doctrine, [information] and values between other armed forces (formally organized or not) and US forces. Engagements are symmetric if forces, technologies, and weapons are similar; they are asymmetric if forces, technologies, and weapons are different, or if a resort to terrorism and rejection of more conventional rules of engagement are the norm.

Source: Department of the Army. "Operations." FM 3-0. June 2001, http://www.dtic.mil/doctrine/jel/service_pubs/fm3_0a.pdf

3. U.S. military doctrine does not accurately address or define the concept of asymmetry. In addition to this failure, US doctrine worsens the effect by consistently using the word to describe other concepts, actions, or terms. The confusing void is found across all services to varying degrees, but it is founded in joint doctrine…the definitions of asymmetry in doctrine are too many, and eventually led the service members to believe that just about anything or everything asymmetric.

Source: Steven D. Pomper. *Asymmetric: Myth in United States Military Doctrine*. Thesis. Durham, NH: University of New Hampshire, 1991. 36-37. ADA428994, http://handle.dtic.mil/100.2/ADA428994; also see Steven Metz and Douglas Johnson III, *Asymmetry and U.S. Military Strategy: Definition, Background, and Stregeic Concepts,* Strategic Studies Institute, 2001, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB223.pdf

4. In formal terms, we can define asymmetry as any military significant disparity between contending parties with respect to the elements of military broadly construed. Asymmetrics invites a study of the fact that elements of military power are never applied in a vacuum, but always in particular political, economic, cultural, religious, psychological, geographic, and climatic contexts that qualify the utility of each element of power and condition the way each acts against the other elements of power.

Source: Lloyd J. Matthews. "Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?" July 1998, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=230

**Authentication**

1. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary* June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

2. A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator. 2. A means of identifying individuals and verifying their eligibility to receive specific categories of information. 3. Evidence by proper signature or seal that a document is genuine and official. 4. In evasion and recovery operations, the process whereby the identity of an evader is confirmed.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Automated Ontologically Based Link Analysis of International Web Logs for the Timely Discovery of Relevant and Credible Information**

A blog search engine which analyzes patterns of importance to the intelligence community [sm]

Blog research may provide information analysts and warfighters with invaluable help in fighting the war on terrorism. Patterns include the content of the blogs as well as what hyperlinks are contained within the blog. Within blogs, hyperlinks act like reference citations in research papers thereby allowing someone to discover the most important events bloggers are writing about in just the same way that one can discover the most important papers in a field by finding which ones are the most cited in research papers.

Source: William J. Sharp. Blogs Study May Provide Credible Information. DoD. *TransFormations*, http://www.defenselink.mil/transformation/articles/2006-06/ta062906b.html and Rory O'Connor, Pentagon Studies Blogs as Terror-Fighting Tool. Alternet July 19, 2006, http://www.alternet.org/columnists/story/39227/

### Automated Trusted Information Exchange (ATIX)

Operated by the Regional Information Sharing Systems®, ATIX is a secure means to disseminate national security or terrorist threat information to law enforcement and other first responders via the ATIX electronic bulletin board, secure Web site, and secure e-mail.

Source: DOJ, Global Justice Information Sharing Initiative, *Criminal Intelligence Glossary of Terms*, *Minimum Criminal Intelligence Training Standards*, Appendix, October 2007, http://www.it.ojp.gov/documents/min_crim_intel_stand.pdf

### Automatic Declassification

1. "Automatic declassification" means the declassification of information based solely upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under this order.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

2. Executive Order 12958, "Classified National Security Information" (the Order), called for a renewed commitment by the Executive branch to the concept of declassification tied to specific deadlines, referred to in the Order as automatic declassification. This direction calls for all 25-year-old and older historically valuable permanent records containing classified national security information to be declassified, exempted, excluded, referred to other interested agencies, or appropriately delayed by December 31, 2006, and each year thereafter, for such records prior to their attaining 25-year-old status. As such, it is important to recognize that December 31, 2006, represents not an end unto itself but rather the beginning of integrating automatic declassification into the fabric of the security classification framework.

Source: Information Security Oversight Office. "Report to the President: An Assessment of Declassification in the Executive Branch." September 21, 2005. http://www.archives.gov/isoo/reports/2005-declassification-report.html

**Autonomy**

*See Data Mining*

Defense Intelligence Agency, Department of Energy, is a large search engine tool that is used to search hundreds of thousands of word documents. Is used for the organization and knowledge discovery of intelligence;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: No;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004. http://www.gao.gov/htext/d04548.html

**Available Publicly**

Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public. In this context "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

Source: DoD. Under Secretary of Defense for Policy. DoD 5240.1-R. Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons. December, 1982: 7. http://www.fas.org/irp/doddir/dod/d5240_1_r.pdf

---

**~ B ~**

**Basic Intelligence**

Factual, fundamental, and relatively permanent information about all aspects of a nation – physical, social, economic, political, biographical, and cultural – which is used as a base for intelligence products in the support of planning, policymaking, and military operations.

Source: Office of Public Affairs, Central Intelligence Agency. *A Consumer's Guide to Intelligence : Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C. : Springfield, VA : National Technical Information Service, [1999?]. SUDOC: PREX 3.2:C 76 PREX 3.2/2:G 94

**Behavioral Advertising**

***See Privacy***

Behavioral advertising matches advertisements to a consumer's interests as determined over time. If a consumer visits several different travel sites before viewing a news site, the consumer might see a behaviorally-targeted travel advertisement displayed on the news page, even though the news page contains no travel content. A traditional behavioral ad network assembles profiles of individual consumers by tracking users' activities on publisher sites within their network. When the consumer visits a site where the ad network has purchased ad space, the ad network collects data about that visit while serving an advertisement based on the consumer's profile. While only a small portion of online ads are currently targeted this way, behavioral advertising is a growing segment of the online advertising industry.

Consumers' behavioral advertising profiles may incorporate many different kinds of data that are not personally identifiable by themselves…

Source: Center for Democracy & Technology (CDT)*, A Primer on Behavioral Advertising*, July 31, 2008, http://cdt.org/publications/policyposts/2008/12, Leslie Harris, Center for Democracy & Technology, Testimony, Senate Commerce, Science & Transportation Committee "Privacy Implications of Online Advertising," July 9, 2008, http://cdt.org/testimony/20080709harris.pdf, CDT, "Online Behavioral Advertising: Discussing the ISP-Ad Network Model,"http://cdt.org/publications/policyposts/2008/15 and Robert M. Topolski, Free Press and Public Knowledge, "NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking," June 18, 2008, http://www.publicknowledge.org/pdf/nebuad-report-20080618.pdf

**Biodefense Knowledge Center (BKC)**

The Biodefense Knowledge Center supports NBACC facility component centers and has its own functions and missions. One is to provide scientific assessments and information to the Homeland Security Operations Center regarding potential bioterrorism events. Another is to be a repository of biodefense information, including genomic sequences for pathogens of concern, the existence and location of vaccines, bioforensics information, and information about individuals, groups, or organizations that might be developing these pathogens. Finally, the BKC aids in assessing potential bioterrorism agents as "material threats" for the purpose of the Project Bioshield countermeasure procurement process.

Once proposed as one of the centers comprising the National Biodefense Analysis and Countermeasures Center (NBACC), dedicated on September 10, 2004, but established separately at Lawrence Livermore National Laboratory, and now appears to be a center independent of the NBACC facility and NBACC program.

Source: Dana A. Shea, The National Biodefense Analysis and Countermeasures Center: Issues for Congress, *CRS Reports for Congress* February 15, 2007, http://www.fas.org/sgp/crs/homesec/RL32891.pdf

Note: The biological weapons convention stipulates that the signatories must not "develop, produce, stockpile, or otherwise acquire or retain" biological weapons, and does not distinguish between offensive and defensive intentions.

**Black**

***See Red***

In the information processing context, black denotes data, text, equipment, processes, systems or installations associated with unencrypted information that requires no emanations security related protection. For example, electronic signals are "black" if bearing unclassified information.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090 "Definitions of Diplomatic Security Terms." November 13, 2003, http://foia.state.gov/REGS/Search.asp

**Black Products**

Products that purport to emanate from a source other than the true one are known as black products. Black products are best used to support strategic plans.

Source: DoD *Psychological Operations*, FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

**Blowback | Blow Back | Information Blowback | Replay**

***See Disinformation, Information Laundering, Prepackaged News***

1. Deception planted abroad by an intelligence agency to mislead people in other countries, then returning to the originating nation, where it misleads that people, or even the government itself. When William Colby, the United States Director of the Central Intelligence Agency testified before the Church Committee in 1977, he admitted

Source: Norman Polmar, and Thomas B. Allen. *Spy Book: the Encyclopedia of Espionage.* New York : Random House Reference, 2004. 2nd ed.

2. Speaking of the Central Intelligence Agency (CIA), Ralph W. McGehee (180-181) reports that CIA intelligence reports and news reports "were frequently similar" Sometimes a newspaper article preceded the intelligence report; sometimes the intelligence report came first; sometimes the two arrived simultaneously. Completeness of detail and accuracy of observation showed the same results. Occasionally and ominously, a cabled intelligence report was identical to a newspaper item. ..Unfortunately there was no mechanism that prevented that disinformation from contaminating and spoiling the CIA's own information files…Occasionally I

could recognize and separate out the CIA-generated articles from others, but more often it was impossible to tell positively whether an item was genuine or planted. Many articles that I kept and filed, that served as background for the studies I wrote, later turned out to be CIA propaganda."

As an example of "information blowback," McGehee (181) writes that during the "Cultural Revolution in China, the Agency's huge radio transmitters on Taiwan broadcast items as if they were continuations of mainland programs. Their broadcasts indicate the revolution was getting out of hand and was much more serious than it actually was. These broadcasts were picked up by the Agency's Foreign Broadcast Information Service (FBIS) and included in its daily booklets of transcriptions from the mainland. From there the information was picked up by other offices of the Agency and reported as hard intelligence…here was a dangerous cycle. Agency disinformation, mistaken as fact, seeped into the files of U.S. government agencies and the CIA itself. It became fixed as fact in the minds of employees who had no idea where it had originated. "

Source: Ralph W. McGehee. *Deadly Deceits: My 25 Years in the CIA*. New York: Sheridan Square Publications, 1983, and Tabassum Zakaria. "U.S. Planting False Stories Common Cold War Tactic." *Reuters* February 25, 2002, http://www.fas.org/sgp/news/2002/02/re022502.html

3. One of the major dangers of disinformation is blowback, in which false information reaches not only its intended target abroad but citizens back home, and the increased interconnectedness of the world is making blowback a greater risk. The short- term consequences vary. In practice, it should not matter a great deal if Joe Sixpack falsely believes the president of Indonesia moonlights as a pornographic actor. On the other hand, there can be policy consequences, as in the Allende case, in which efforts to discredit him in Chile might have affected American public opinion and support for the Nixon's Administration's Chile policy.

Source: Thomas C. Ellington. "Won't Get Fooled Again: The Paranoid Style in the National Security State." *Government and Opposition* 38 (2003): 436-455.

4. Possibilities of blowback against the United States should always be in the back of the minds of all CIA officers involved in this type of operation. Few, if any, operations are as explosive as this type. This fact makes it imperative that the best trained and experienced officers who can be found be assigned.

Source: CIA Clandestine Service History. "Overthrow of Premier Mossadeq of Iran, November 1952-August 1953," March 1954. Appendix E. "Military Critique: Lessons Learned from TPAJAX Military Planning RE: Aspects of Coup d'Etat." 21, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB28

5. …if one is practicing deception in order to affect public or international opinion, the "blow back" from loss of credibility can easily prove quite damaging. This consideration gained international attention when it was revealed in early 2002 that DoD had established an "Office of Strategic Influence." While it was quickly asserted that this organization would not be deceptive, media sources implied that foreign media might be provided with manipulated information. This set off a flurry of charges and denials and the eventual; closing of the office. Even the appearance of deception can be expensive.

Source: Joseph W. Caddell. "Deception 101-Primer on Deception." December 2004, http://www.fas.org/irp/eprint/deception.pdf

6. The term "blowback," which officials of the Central Intelligence Agency first invented for their internal use, is starting to circulate among students of international relations. It refers to the unintended consequences of policies that were kept secret from the American people. What the daily press reports as the malign acts of "terrorists" or "drug lords" or "rogue states" or "illegal arms merchants" often turn out to be blowback from earlier American operations (8). Blowback itself can lead to more blowback, in a spiral of destructive behavior (10).

In a sense blowback is simply another way of saying that a nation reaps what it sows…as a concept, blowback is obviously most easy to grasp in its most straightforward manifestation. The unintended consequences of American policies and acts in country X are a bomb at an American embassy in country Y or a dead American in country Z…because we live in an increasingly interconnected international system, we are all in a sense, living in a blowback world. Although the term originally applied only to the unintended consequences for *Americans* of American policies, there is every reason to widen its meaning. Whether, for example, any unintended consequences of the American policies that fostered and then heightened the economic collapse of Indonesia in 1997 ever blow back to the United States, the unintended consequences for Indonesians have been staggering levels of suffering, poverty, and loss of hope. (17-18)

Source: Chalmers Johnson. *Blowback: the Costs and Consequences of American Empire.* New York: Metropolitan Books, 2000. 3-33.

7. (DOD, NATO) 1. Escape, to the rear and under pressure, of gases formed during the firing of the weapon. Blowback may be caused by a defective breech mechanism, a ruptured cartridge case, or a faulty primer. 2. Type of weapon operation in which the force of expanding gases acting to the rear against the face of the bolt furnishes all the energy required to initiate

the complete cycle of operation. A weapon which employs this method of operation is characterized by the absence of any breech-lock or bolt-lock mechanism.[26]

Source: DoD. *DoD Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

8. Perhaps the most disquieting danger in the CIA use of the media lies in the phenomenon of blow back or replay, that is the return to the United States of Agency propaganda planted abroad – the brainwashing of the American people by one of their own secret intelligence agencies, to put it in harsh, Orwellian terms. [Note: the Church Committee files contain reports of blowback & the "Aspin Committee," United States. Congress. House. Permanent Select Committee on Intelligence. Subcommittee on Oversight. *The CIA and the Media : hearings before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence, House of Representatives*, Ninety-fifth Congress, first and second sessions. Washington : U.S. Government Printing Office, 1978. Y 4.In 8/18:C 33]

Source: Loch K. Johnson. *America's Secret Power: the CIA at Home and Abroad.* New York: Oxford University Press, 1989. 197.

**Blue Paper**

April 11, 1940 FBI Director Hoover institutes a special reporting procedure governing senior FBI officials' written communications about especially sensitive and administrative matters. Such reports were to be prepared on colored paper (first blue and then pink) to preclude their serialization in the FBI's central records system. Hoover terminated this reporting procedure in 1950. Thereafter, FBI officials reported such information in "informal" memoranda (plain white nonletterhead paper), which were then maintained in office files until destroyed.

Source: Athan Theoharis, ed. *The FBI: A Comprehensive Reference Guide*. Phoenix: Oryx Press, 1998. 366.

**Born Classified**

***See Classification Levels, Classified at Birth, Nuclear Secrecy, Restricted Data***

1. According to Richard G. Hewlett, throughout its existence from 1946-1975, the United States Atomic Energy Commission (AEC) consistently relied upon the born classified concept in administering its statutory authority to control the dissemination of classified information. Certain types of information were "born classified" whether that information was generated in an official government project, or in the mind of a private citizen working in his own home. Moreover, the AEC and staff almost never used the words "born classified;" the

[26] Thanks to M.R. for suggesting this definition.

concept, however, “grew quite naturally out of the American experience in World War II. The atomic bomb project was the best kept secrets of the war.”

The first draft of the atomic energy bill, introduced in the Senate December 20, 1945 by Senator Brien McMahon, gave emphasis to the distinction between scientific and related technical information as linked to atomic energy, production and use of fissionable materials. Over the course of discussions regarding the bill, the original Section 9 (now 10) of the McMahon bill evolved from “Dissemination of Information” to “Control of information” abandoning the convolutions between “scientific” and “related technical” information for a special category of “Restricted Data,” or RD. RD is “all data concerning the manufacture or utilization of atomic weapons , production of fissionable materials or the use of fissionable material in the production of power, but shall not include any data which the commission from time to time determines may be published without adversely affecting the common defense or security.”

Hewlett (175-176) believes the category of RD recognized the existing situation that all information related to these above-mentioned aspects of nuclear technology, (including the controversial and nebulous category of “privately generated information”), was already classified, and could be declassified only by positive action on behalf of the AEC; herein lie the “seed of the ‘born classified’ concept.” In other words, anything that was classified as RD meant that“ everything encompassed by it was [therefore] automatically classified.”

Source: Richard G. Hewlett. “The ‘Born-Classified’ Concept in the U.S. Atomic Energy Commission.” May 1980. 173-187. In United States. Congress. House. Committee on Government Operations. *The Government's Classification of Private Ideas: Thirty-fourth Report*. 96th Congress, 2d session, House of Representatives; no. 96-1540. Washington: GPO, 1980. SUDOC: X 96-2:H.rp.1540

2. Now let us get back to the information that is born classified. This phenomenon, too, is representative of a great upheaval. We were invaded, as it were, by a tribe of people peculiar in their possession of the fissioning atom. Peculiar, too, in that they could be trusted to keep that knowledge a tribal secret. And so, because man’s welfare – indeed man’s survival- was deemed to depend on it, the tribal knowledge was decreed to be Restricted Data, inaccessible to people outside the tribe except after a special initiation ceremony, known mysteriously as Q. [Q clearance]

And so we were swept into the new age; and along with a flood of new knowledge, new hopes, and new perils we had to cope with a new concept in controlling information.

Source: Donald Woodbridge. "Some Thoughts on Classification in the AEC." *National Classification Management Society Journal.* Papers from the National Seminar 6th VI no. 1, 1971. 22-33.

3. Speaking of the Morland case (*U.S. v. The Progressive, Inc.* , 467 *F. Supp.* 990), McCloskey (188) notes: "the problem lies with the "Born Secret" concept contained in the Atomic Energy Act of 1954, which has three elements: 1. Classification procedures and policies of the Department of Energy, 2. The ambiguity of the present law as it is being interpreted by the Energy and Justice Departments, and 3. Increasing public dispersion of scientific data bearing on construction and use of weapons which can destroy mankind…"

Source: Hon. Paul N. McCloskey, Jr. "Additional Views." 188-193. In United States. Congress. House. Committee on Government Operations. *The Government's Classification of Private Ideas: Thirty-fourth Report*. 96th Congress, 2d session, House of Representatives; no. 96-1540. Washington: GPO, 1980. SUDOC: X 96-2:H.rp.1540

4. Technically, according to the "born secret" clause of the Atomic Energy Act, even if I had gotten all three concepts wrong, my story could still have been classified, because if it's about nuclear energy, and if it hasn't been declassified, then it's classified, even if it's not true.

Source: Howard Morland. "The Holocaust Bomb: a Question of Time." FAS e-prints, February 5, 2003. http://www.fas.org/sgp/eprint/morland.html

5. The government claimed the "classified at birth' concept to be necessary to "ensure that sensitive information would not be divulged before the United States had an opportunity to assess its importance and take appropriate classification action."

Source: Alexander DeVolpi et al. *Born Secret: the H-bomb, the Progressive Case and National Security.* New York: Pergamon Press, 1981, 59; also see William Burr, Thomas S. Blanton, and Stephen I. Schwartz. "The Costs and Consequences of Nuclear Secrecy." In Stephen Schwartz, (ed.) *Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons Since 1940*. Brookings Institute, 1998. 433-483.

6. The Atomic Energy Act (the Act) has been with us since 1946. No law passed before or since gives the government such sweeping authority to keep information secret. Under the information control provisions of the Act, practically all information related to nuclear weapons and nuclear energy is "born classified" : it is a government secret as soon as it comes into existence. No governmental act is necessary to classify information. Moreover, the information, defined as Restricted Data, remains secret until the government affirmatively determines that it may be published. (163)

A question latent in the language of the Act is whether privately developed or privately generated atomic energy information – information developed or generated without government funds and without access to classified government documents – is Restricted Data, and thus subject to the Act.

Source: Mary M. Chen. "The Progressive Case and the Atomic Energy Act : Waking to the Dangers of Government Information Controls." *George Washington Law Review* 48 no. 2 (1979-1980): 163-311.

7. The definition of RD contained in the AEA [Atomic Energy Act] has been interpreted to mean that all information falling within the RD definition is automatically classified or "born classified." When the AEA was written, this was effectively true and most of this type of information was classified. Now, this all-encompassing definition for RD has been reduced by nearly fifty years of declassification actions to a core of information. Information which remains classified as RD relates primarily to nuclear weapons design, or the use or acquisition of nuclear weapons or nuclear material, with nuclear science and much nuclear technology excluded because it is no longer classified. Only five areas of nuclear technology still contain information classified as RD or FRD. Each of these broad areas contains specific information that is still classified and other information that has been declassified. Identifying whether specific information is classified in these areas requires technical expertise and reference to a classification guide. The nuclear field is now quite mature; any new information is likely to be either further detail in an area for which classification guidance is already well established, or characteristics of a new weapon design operating outside the envelope of its predecessors. In the latter case, the classification of such information is not automatically prescribed, but is determined by authorized officials by application of specific criteria. This procedure de-emphasizes, but does not abolish, the "born classified" concept.

Source: Department of Energy. 10 CFR Part 1045 "Information Classification; Proposed Rule." *Federal Register* 62 no. 10 (January 15, 1997), at FAS, http://www.fas.org/sgp/clinton/doereg.html

**Brevity Codes**

A brevity code is a code which provides no security but which has as its sole purpose the shortening of messages rather than the concealment of their content. Approved brevity codes may be used when preparing military records, publications, correspondence, messages, operation plans, orders, and reports.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004., http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545-b.htm

**Briefing**
Presentation, usually oral, of information. The preparation of an individual for a specific operation by describing the situation to be encountered, the methods to be employed, and the objective.

Source: Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C. : Springfield, VA : National Technical Information Service, [1999?]. SUDOC: PREX 3.2:C 76 PREX 3.2/2:G 94

**Browsing**
Act of searching through IS (information system) storage to locate or acquire information, without necessarily knowing the existence or format of information being sought.

Source Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary* June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Burden**
The impact on the public of an information collection or recordkeeping; specifically:
Burden means the total time, effort, or financial resources expended by persons to generate, maintain, retain, or disclose or provide information to or for a Federal agency, including:
(i) Reviewing instructions;
(ii) Developing, acquiring, installing, and utilizing technology and systems for the purpose of collecting, validating, and verifying information;
(iii) Developing, acquiring, installing, and utilizing technology and systems for the purpose of processing and maintaining information;
(iv) Developing, acquiring, installing, and utilizing technology and systems for the purpose of disclosing and providing information;
(v) Adjusting the existing ways to comply with any previously applicable instructions and requirements;
(vi) Training personnel to be able to respond to a collection of information;
(vii) Searching data sources;
(viii) Completing and reviewing the collection of information; and
(ix) Transmitting, or otherwise disclosing the information.

Source. Office of Management and Budget. 5 CFR 1320. "Controlling Paperwork Burdens on the Public." http://www.gpoaccess.gov/cfr/index.html

**Bureau of International Information Programs (IIP)**
***See Counter-Information Team, Information Exploitation, Propaganda, Public Diplomacy***
IIP delivers America's message to the world through a number of key products and services. The

outreach is created strictly for international audiences, such as international media, government officials, opinion leaders, and the public in more than 140 countries around the world.

> Delivers America's message to the world, counteracting negative preconceptions, maintaining an open dialogue, and building bridges of understanding to help build a network of communication, promote American voices, and forge lasting relationships in international communities.
>
> Delivers clear and meaningful U.S. policy information and articles about U.S. society in the languages that attract the largest number of viewers -- English, Arabic, Chinese, French, Persian, Russian, and Spanish.
>
> Produces news articles, electronic and print publications, which provides context to U.S. policies, as well as products on U.S. values, culture, and daily life that serves as a window on positive American values.

Source: U.S. State Department. Bureau of International Information Programs,http://www.state.gov/r/iip/

**Bureaucratic Slippage**

The tendency for broad policies to be altered through successive reinterpretation, such that the ultimate implementation may bear little resemblance to legislated or other broad statements of policy intent The net result, we suggest, can resemble the childhood game in which a "secret" is whispered to one person, who then whispers it to the next, and so on; the eventual secret, or the eventual implementation of the policy, can prove to have very little resemblance to the statement that started the process (p.222).

Source: William R. Freudenburg and Robert Gramling, "Bureaucratic Slippage and Failures of Agency Vigilance: The Case of the Environmental Studies Program *Social Problems* 41 no. 2 (1994):214-239.

**Bye | Byeman | Byeman Special Handling (BSH)**

***See Sensitive Compartmentalized Information***

1. Unclassified term that describes sensitive programs and operational data.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

2. BYEMAN Compartmentation Restructure Commissioned by: DNRO November 1993. Conducted by: Joint Government and Industry Review Team Purpose: Create security environment based on need-to-know that enhances efficiencies, eliminates duplication, promotes sharing of technology assets

Source: Defining the Future of NRO for the 21st Century. August 1996, http://www.fas.org/irp/nro/jeremiah_9.htm

3. This directive replaced the original June 1962 DoD Directive on the NRO, and remains in force today. The directive specifies the role of the Director of the NRO, the relationships between the NRO and other organizations, the director's authorities, and security. It specified that documents or other material concerning National Reconnaissance Program matters would be handled within a special security system (known as the BYEMAN Control System).

Source: National Security Archive. Department of Defense Directive Number TS 5105.23. 27 March 1964, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/08-01.htm

---

## ~ C ~

### Call-identifying Information

Section 102(2) of CALEA [Communications Assistance for Law Enforcement Act] defines call-identifying information as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."

Source: CALEA Implementation Unit (CIU), Electronic Surveillance Technology Section, Operational Technology Division, Federal Bureau of Investigation, http://www.fbi.gov/hq/otd/otd.htm, Also see Ask CALEA. http://www.askcalea.net/faqs.html#03

### Carnivore | DCS 1000

*See Altivore, DCSNET*

1. Carnivore is software that runs under Windows NT with Service Pack 3 or better that is designed to capture network traffic, based on a series of options, and save that traffic to a storage medium such as a hard disk [memo redacted].

Source: Electronic Privacy Center (EPIC). Carnivore Purpose." http://epic.org/privacy/carnivore/foia_documents.html and FBI Report to Congress on Use of Carnivore/DCS 1000. http://www.epic.org/privacy/carnivore/2003_report.pdf

2. Carnivore is a system which we are counting on to help us in critical ways in combating acts of terrorism, espionage, information warfare, hacking, and other serious and

violent crimes occurring over the Internet, acts which threaten the security of our Nation and the safety of our people; a special purpose electronic surveillance tool…

Source: Testimony of Donald M. Kerr, Assistant Director, Laboratory Division, FBI.
United States Senate. Committee on the Judiciary. September 6, 2000. "Carnivore Diagnostic Tool."
http://www.fbi.gov/congress/congress00/kerr090600.htm

### Case Management Data Mart

*See Data Mining*

Department of Homeland Security. Assists in managing law enforcement cases, including Customs cases. Reviews case loads, status, and relationships among cases;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: Yes;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

### Categorical Exclusion

*See Environmental Impact Statement, Twilight Information*

Created under the National Environmental Policy Act (NEPA),[27] and signed into law on January 1, 1970. Categorical exclusion "means a category of actions which do not individually or cumulatively have a significant effect on the human environment and which have been found to have no such effect in procedures adopted by a Federal agency in adoption of these procedures (CFR Section 1507.3) and for which, therefore, neither an environmental assessment nor an environmental impact statement is required."

Source: EPA. "Protection of the Environment." 40 CFR 1508.4, http://www.gpoaccess.gov/CFR/index.html

### Categories of Data

In the context of perception management and its constituent approaches, data obtained by adversary individuals, groups, intelligence systems, and officials. Such data fall in two categories: a. information--A compilation of data provided by protected or open sources that would provide a substantially complete picture of friendly intentions, capabilities, or activities. b. indicators--Data derived from open sources or from detectable actions that adversaries can

[27] Cornelius M. Kerwin (60) characterizes NEPA an "information statute." (*Rulemaking:How Government Agencies Write Law and Make Policy*. Washington, D.C.: CQ Press, 1994).

piece together or interpret to reach personal conclusions or official estimates concerning friendly intentions, capabilities, or activities. (Note: In operations security, actions that convey indicators exploitable by adversaries, but that must be carried out regardless, to plan, prepare for, and execute activities, are called "observables.") See also operations security.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Category**

Restrictive label applied to classified or unclassified information to limit access.

Source: Committee for National Security Systems (CNSS). Instruction 4009. National Information Assurance Glossary June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Caveated Information | Caveat**

***See Classification Markings / Control Markings, D.C.ID 1/7, "Security Controls on the Dissemination of Intelligence Information***

1. Information subject to one of the authorized control markings under Section 9 of DCID 1/7, "Security Controls on the Dissemination of Intelligence Information."

Source: Director of Central Intelligence "Directive 1/7 Security Controls on the Dissemination of Intelligence Information." June 30, 1998, http://www.fas.org/irp/offdocs/D.C.id1-7.html

2. A designator used with a classification to further limit the dissemination of restricted information. (JP 3-07.4)

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Censorship**

***See Armed Force Censorship, Civil Censorship, Field Press Censorship, National Censorship; Primary Censorship, Prisoner of War Censorship, Secondary Censorship.***

1. A form of surveillance; all socially structured proscriptions or prescriptions which inhibit or prohibit dissemination of ideas, information, images and other messages through which a society's channels of communication whether these obstructions are secured by political, economic, religious, or other systems of authority. It includes both overt and covert proscriptions and prescriptions.

Source: Sue Curry Jansen. *Censorship: The Knot that Binds Power and Knowledge*. New York: Oxford University Press, 1991.

2. Advance censorship is the most serious attack on freedom of expression possible. It puts the burden of proof upon the person who desires to communicate information instead of upon the government attempting to suppress it. It forces the defendant to comply with the censor or to be found in violation of the law.

Source: Rep. Ted Weiss, 20th District New York. Letter to Richard Preyer, Chairman, Government Information and Individual Rights Subcommittee. In United States. Congress. House. Committee on Government Operations. Subcommittee on Government Information and Individual Rights. *The Government's Classification of Private Ideas*. Hearings before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-sixth Congress, second session, February 28, March 20, and August 21, 1980. 785. SUDOC: Y 4.G 74/7: G 74/5

### Russian definitions of censorship

1. *Tsenzura.* The examination of texts by an authorized state agency with the aim of approving or banning their publication in the open press or their broadcast by radio or television; the examination of private postal correspondence to determine the political bias of a text and its ideological content, and removing the possibility that information constituting a state or military secret might be divulged.

Also the scrutiny of manuscripts by open civil publishing houses, and the task of allowing or forbidding the works of these houses to be sent abroad under the responsibility of the Chief Directorate for the protection of State Secrets in Print under the USSR Council of Ministers and local branches.

Source: Vasily Mitrokhin, ed. *KGB Lexicon: The Soviet Intelligence's Officer's Handbook*. London: Frank Cass, 2002.

2. *Tsenzura voyennaya*, or military censorship same as above, under the direction of the USST Ministry of Defence.

Source: Vasily Mitrokhin, ed. *KGB Lexicon: The Soviet Intelligence's Officer's Handbook*. London: Frank Cass, 2002.

### Central Foreign Policy File

An automated database that contains texts of telegrams and abstracts of written documents about Department policies dating back to 1973.

Source: U.S. Department of State. *Foreign Affairs Manual*. 5FAM420, "Organizing, Maintaining and Protecting Records." (5FAM421.2), http://www.state.gov/m/a/dir/regs/

## CIA Crypts

The Review Board released some CIA "crypts " — codewords for operations and individuals. The Review Board also generally released CIA "digraphs"—the first two letters of a crypt that link a particular crypt to a particular location. CIA often created crypts to refer to other U.S. government agencies; for example, the FBI was "ODENVY." The Review Board made a blanket decision to release all U.S. government crypts. The Review Board nearly always released CIA crypts where those crypts denoted operations or individuals relating to Mexico City or Cuba. (The digraph for Mexico City was "LI," and for Cuba, it was "AM.") For all other crypts, the Review Board protected the digraph and released the remainder of the crypt. The Review Board established a few exceptions, and where exceptions applied, the Board required CIA to provide crypt-specific evidence of the need to protect. (p.51-52)

HTLINGUAL is the crypt for CIA's mail opening and mail cover program for 1952 to 1973. The CIA reported to the Review Board that it destroyed most of its formal HTLINGUAL records in 1990 at the direction of CIA's Office of General Counsel. (p.83)

Source: Assassination Review Board, *Final Report of the Assassination Records Review Board*, September 1998, http://www.archives.gov/research/jfk/review-board/report/

## CIA File Numbers

The CIA organizes many of its files by country and assigns "country identifiers" within particular file numbers. The Review Board released nearly all CIA file numbers that referred to Mexico City. The Review Board protected the "country identifiers" in CIA file numbers for all other countries with the exception of country identifiers "15" and "19." The Review Board generally released all CIA "201" or "personality" file numbers where the files related to the assassination.

Source: Assassination Review Board, *Final Report of the Assassination Records Review Board*, September 1998, http://www.archives.gov/research/jfk/review-board/report/

## CIA Records Search Tool (CREST)

1. CIA database of declassified intelligence documents. The database, searchable by title, data, and text content, includes Directorate of Operations reports on the role of intelligence in the post WW-II period; material on the creation, organization, and role of the CIA within the U.S. Government; a collection of foreign scientific articles, ground photographs and associated reference materials; and the CIA's first release of motion picture film.

Source: NARA, "Searchable Databases in the Library," http://www.archives.gov/research/alic/tools/online-databases.html#m4; the Finding Aid is located here: http://www.foia.cia.gov/search_archive.asp

2. The CREST system is the publicly-accessible repository of the subset of CIA records reviewed under the 25-year program in electronic format (manually reviewed and released records are accessioned directly into the National Archives in their original format). Over 10 million pages have been released in electronic format and reside on the CREST database, from which researchers have printed almost a million pages. To use CREST, a researcher must physically be present at the National Archives, College Park, Maryland. Recognizing this presents an obstacle to many researchers, we have been investigating ways to improve researcher knowledge of and access to CREST documents.

Source: CIA, "25-Year Program Archive Search," http://www.foia.cia.gov/search_archive.asp

### CIA Sluglines

"Sluglines" are CIA routing indicators, consisting of two or more crypts, that appear above the text in CIA cables. (p.52)

An example of a CIA slugline is " RYBAT GPFLOOR." "RYBAT" is a CIA crypt that meant "secret" and GPFLOOR was the crypt that CIA gave Lee Harvey Oswald during its post-assassination investigation. (p.53)

Source: Assassination Review Board, *Final Report of the Assassination Records Review Board*, September 1998, http://www.archives.gov/research/jfk/review-board/report/

### CIPAV (Computer and Internet Protocol Address Verifier)

CIPAV may cause any computer – wherever located – that activates any CIPAV authorized by this Court ("an activating computer") to send network level messages containing the activating computer's IP address and/or MAC address, or other environmental variables, and certain registry-type information to a computer controlled by the FBI. (p.3)

Source: United States District Court, Western District of Washington, Application and Affidavit for Search Warrant, June 12, 2007, (thanks to Politech for obtaining the doc), http://politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf and http://politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf

### Cipher Text

Enciphered information.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

### Civil Censorship

***See Censorship***

Censorship of civilian communications, such as messages, printed matter, and films entering, leaving, or circulating within areas or territories occupied or controlled by armed forces

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Civil Censorship Detachment**

A unit of the Supreme Commander of the Allied Powers' (SCAP) Press, responsible for controlling information, including the media in postwar Japan.

Source: Gordon W. Prange Collection, University of Maryland Libraries, http://www.lib.umd.edu/prange/html/introduction.jsp#civil; Gar Alperovitz, *The Decision to Use the Atomic Bomb and the Architecture of an American Myth* [esp. chapter 48, 'Censorship and Secrecy," Knopf, 1995]; check with your local library to see if it subscribes to the Prange database, http://www.proquest.com/en-US/catalogs/collections/detail/Prange-Collection.shtml

**Clandestine Operation**

A secret intelligence collection activity or covert political, economic, propaganda, or paramilitary action conducted to ensure the secrecy of the operation.

Source: Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C.: Springfield, VA: National Technical Information Service, [1999?]. SUDOC: PREX 3.2: C 76 and PREX 3.2/2: G 94

**Classification | Security Classification**

1. The act or process by which information is determined to be classified information.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html[28]

2. An so I daresay, CLASSIFICATION began to take on its security connotations as it was recognized that information can and should be put into different classes depending on the degrees of protection required. In the minds of most of us, classified information has come to

[28] The Russian Federation also has an elaborate system of classification; see Pike and http://www.fas.org/irp/world/russia/class.htm and Maret, *Formal and Informal Restrictive Information Categories in the FSU/Russian Federation* http://www.fas.org/irp/world/russia/maret.pdf

mean primarily information that the law requires us to protect, rather than information that has been put into a particular class. This semantic confusion doesn't bother us very much ordinarily, but it becomes important when we are considering the mystique of Restricted Data and when we choose to regard the phrase "born classified as other than a metaphor."

Source: Donald Woodbridge. "Some Thoughts on Classification in the AEC." *National Classification Management Society Journal.* Papers from the National Seminar 6th VI no. 1 1971. 22-33.

3. The process of determining and identifying the information we need to protect in the interests of national security – the information we need to conceal from the enemies and potential enemies of the United States.

Source: DOE. *Understanding Classification***.** Washington, D.C.: U.S. Dept. of Energy, Assistant Secretary for Defense Programs, Office of Classification, 1987. E 1.15:0007/1 and *Manual for Identifying Classified Information*, August 28, 2007, http:// www.doeal.gov/OSTSSC/docs/DOEM47511B.pdf

4. A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. There are three such categories. a. top secret--National security information or material that requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. b. secret--National security information or material that requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. c. confidential--National security information or material that requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

6. Three Special Types of Classification:

a. Classification by association is a situation where the mere fact that two items of information are related is in itself classified;

b. Two or more items of unclassified information, when put together create some additional factor which warrants classification. This is termed "classification by compilation."

c. Masking is the act of classifying one piece of information solely to protect a separate item of information.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

7. Current Classification System–Cumbersome and Confusing

The classification system is more complex than necessary. Classification is inherently subjective and the current system inappropriately links levels of classification with levels of protection. The current classification system starts with three levels of classification (Confidential, Secret, and Top Secret), often referred to collectively as collateral. Layered on top of these three levels are at least nine additional protection categories. These include Department of Defense Special Access Programs (DoD SAPs), Department of Energy Special Access Programs, Director of Central Intelligence Sensitive Compartmented Information Programs (DCI SCI), and other material controlled by special access or "bigot" lists, (The term "bigot" is said to have been coined during World War II, with reference to the controls on information sent TO GIBRALTAR, or TOGIB, reversed as BIGOT), such as the war plans of the Joint Chiefs of Staff and the operational files and source information of the CIA Operations Directorate. Further complicating the system are restrictive markings and dissemination controls such as ORCON (dissemination and extraction of information controlled by originator), NOFORN (not releasable to foreign nationals), and "Eyes Only."

Source: Joint Security Commission. "Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence." February 28, 1994, http://www.fas.org/sgp/library/jsc/

8. Patents are classified (*organized*) in the U.S. by a system using a 3 digit class and a 3 digit subclass to describe every similar grouping of patent art. A single invention may be described by multiple classification codes. See the Manual of Patent Classification.

Source: U.S. Patent and Trademark Office. Glossary.
http://www.uspto.gov/main/glossary/index.html#c

9. Limiting the quantity of security classified information has been thought to be desirable for a variety of important reasons: (1) promoting an informed citizenry, (2)

effectuating accountability for government policies and practices, (3) realizing oversight of government operations, and (4) achieving efficiency and economy in government management.

Source: Harold C. Relyea, "Security Classified and Controlled Information: History, Status, and Emerging Management Issues. CRS Report to Congress RL 33494, updated February 11, 2008, http://www.opencrs.com

10. See the ISOO *Annual Report to the President* for classification and declassification statistics, http://www.archives.gov/isoo/reports/; for classification costs per EO Executive Order 12958 and 12829, see ISOO's *Report on Cost Estimates for Security Classification Activities.* However, 2007 costs are reported in the *Annual Report*, 2007 ("…the Government cost estimate for FY 2007 is $8.65 billion, which is a $415 million, or 4.8 percent increase, above the cost estimates reported for FY 2006. The industry estimate is up by $24.6 million. This makes the total FY 2007 cost estimate for Government and industry $9.91 billion, which is $439 million more (4.6 percent) than the total FY 2006 cost estimate for Government and industry. The largest increase came from the Physical Security category…p. 29, http://www.archives.gov/isoo/reports/2007-annual-report.pdf). As per the *Annual Report,* 2008, costs will be published separately; see the May 19, 2008 *Information Security Oversight Office's (IS00) Cost Report for Fiscal Year 2008,* http://www.fas.org/sgp/isoo/2008costs.pdf

## Classification Authority

The authority to classify information originally may be exercised only by: (1) the President and, in the performance of executive duties, the Vice President; (2) agency heads and officials designated by the President in the *Federal Register*..."

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html and White House-ISOO. "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," December 29, 2005 & February 3, 2006, http://www.state.gov/m/ds/clearances/60321.htm

## Classification Block

EO 12958 requires each classified document and message to be marked with certain information about the source or authority for classification, duration of classification, etc. This information is usually located on the face of a classified document or the end of a classified message, and is termed a "classification block."

Source: Defense Intelligence Agency. Office of Security and Counterintelligence, Policy and Security Awareness Branch. *Desk Reference Guide to Executive Order 12958, as Amended, Classified National Security Information.* April 2004.

## Classification by Compilation

***See Classification***

Two or more items of unclassified information, when put together create some additional factor which warrants classification. This is termed "classification by compilation."

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001. http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf and Arvin S. Quist. *Classification of Compilations of Information.* June 1991, http://www.fas.org/sgp/library/compilations.pdf

**Classification Category 29**

***See Classification Markings / Control Markings, National Security Information***

1. Types of information and activities eligible for classification and nondisclosure.

Source: Jason Program Office, Mitre Corporation. "Horizontal Integration: Broader Access Models for Realizing Information Dominance." http://www.fas.org/irp/agency/DoD/jason/classpol.pdf

2. One of three kinds of information; i.e., Restricted Data, Formerly Restricted Data, or National Security Information.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

3. Clinton Executive Order 12958 "Classified National Security Information," established policy and guidelines on classification of national security information, and is amended by Bush Executive Order 13292 (March 25, 2003) in order to "prescribe a uniform system for classifying, safeguarding and classifying national security information relating to defense against transnational terrorism."

Both EO 12958 and EO 13292 outline specific categories of information that "shall not be considered for classification unless it concerns" can be classified by an "authorized original classifier." The Bush EO, moreover, added language related to terrorism, below:

Military plans, weapons systems, or operations;
Foreign government information;
Intelligence activities (including special activities), intelligence sources or methods, or

[29] For Russian classification categories see John Pike's "Classification Levels Used by the Russian Federation," and Maret's "Formal and Informal Restrictive Information Categories in the FSU/Russian Federation." FAS, http://www.fas.org/irp/world/russia/class.htm

cryptology;
Foreign relations or foreign activities of the United States, including confidential sources;
Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
United States Government programs for safeguarding nuclear materials or facilities;
Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
Weapons of mass destruction.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.4 and Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

4. A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required. There are three such categories.

TOP SECRET -- National security information or material that requires the highest degree of protection and the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

SECRET -- National security information or material that requires a substantial degree of protection and the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

CONFIDENTIAL -- National security information or material that requires protection and the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

Source: DoD. *DoD Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

### Classification Challenge

Authorized holders of information classified by the Department who, in good faith, believe that specific information is improperly classified or unclassified are encouraged and expected to challenge the classification status of the information. The challenge need not be more than a question as o why the information is or is not classified, or is classified at a certain level. No retribution or other negative action shall be taken for presenting a challenge.

Source: United States. Department of Justice. Justice Management Division. Information Security Policy Group. Classified national security information. Washington, D.C.: U.S. Dept. of Justice, Justice Management Division, Security and Emergency Planning Staff: Information Security Policy Group, 1998. SUDOC: J1.2:SE2/5

### Classification Guides

***See Classification Markings / Control Markings***

1. Under Executive Orders 12958 and 13292 "Classified National Security Information," and Further Amendment to Executive Order 12958, as Amended, Classified National Security Information," respectively, agencies with original classification authority are responsible for the creation of classification guides "to facilitate the proper and uniform derivative classification of information."

Classification guides are a"documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element." In various agencies that constitute the IC, guides themselves are considered classified material.

Within the Department of Energy (DOE) there are three types of classification guides: *Policy Guides* (cover DOE's classification policy), *Program Guides* (which implement policy as it applies to programs), and *Local Guides* (cover detailed operations within programs).

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 ; Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security

Information." http://www.archives.gov/federal-register/executive-orders/2003.html; DOE. Understanding Classification. Washington, D.C.: U.S. Dept. of Energy, Assistant Secretary for Defense Programs, Office of Classification, 1987, E 1.15:0007/1; National Defense. 32 CFR 2001.15 http://www.gpoaccess.gov/cfr/index.html and AR 380-5, Appendix G "Security Classification Guide Preparation." http://www.fas.org/irp/doddir/army/ar380-5/ag.htm

2. A "Control Markings Register" (Intelligence Community (IC) Classification and Control Markings Register and the CIA National Security Classification Guide) includes a list of the authorized terms that may be used to mark classified materials; also prescribes the exact format for their display. Omitted from the register are certain agency-unique and sensitive markings. Maintained by the Controlled Access Program Coordination Office (CAPCO) of the Community Management Staff (CMS).

Source: "Intelligence Community Classification and Control Markings Implementation." http://www.fas.org/sgp/othergov/icmarkings.ppt and 2006-700-10: Intelligence Community Update to DCID 6/11, "Controlled Access Program Oversight Committee."

3. Developed by the Army G-2, online tutorial at http://www.dami.army.pentagon.mil/offices/dami-cd/security.asp

Source: Standardized Methodology for Making Classification Decisions," Office of the Army Deputy Chief of Staff, G-2, October 25, 2006, http://www.fas.org/sgp/othergov/dod/methodology.pdf

**Classification Level(s)**

***See Classification, Classification / Security Classification***

1. A classification level is assigned to information owned by, produced by or for, or controlled by the United States government.

Source: Office of Justice Programs. Department of Justice. *The National Criminal Intelligence Sharing Plan v.1.0.* October 2003, http://it.ojp.gov/documents/200507_ncisp.pdf

2. A designation assigned to specific elements of information based on the potential damage to national security if disclosed to unauthorized persons. The three levels in descending order of potential damage are Top Secret, Secret, and Confidential.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

**There are Three levels of Classified Information**:[30]

1. Top Secret

The highest classification level applied to information, whose unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security."

Source: NARA. Reagan EO 12356 "National Security Information." http://www.archives.gov/federal-register/executive-orders/1982.html and Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

Top-Secret Access Authorizations or Clearances are based on background investigations conducted by OPM or another Government agency, which conducts personnel security investigations. Top Secret clearances permit an individual to have access on a need-to-know basis to Top Secret, Secret, and Confidential levels of National Security Information and Formerly Restricted Data as required in the performance of duties. Top Secret is applied to information (RD, FRD, or NSI).

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 , Los Alamos National Lab. "Definitions," http://www.hr.lanl.gov/SCourses/All/PortionMarking/define.htm , Federation of American Scientists, http://www.fas.org/irp/DoDdir/doe/o5631_2c/o5631_2ca2.htm and Energy. 10 CFR 1045, http://www.gpoaccess.gov/CFR/index.html

2. Secret

Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe; the classification level between Confidential and Top Secret applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Secret is applied to information (RD, FRD, or NSI).

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 , Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information," http://www.archives.gov/federal-register/executive-orders/2003.html, Los Alamos

[30] For an examination of classification and codeword practices in the UK, Australia, and New Zealand, see Jeffrey Richelson and Desmond Ball's *The Ties That Bind: Intelligence Cooperation between the UKUSA Countries, the United Kingdom, the United States of America, Canada, Australia, and New Zealand*. Boston: Allen & Unwin,1985.

National Lab. "Definitions," http://www.hr.lanl.gov/SCourses/All/PortionMarking/define.htm and Energy.
10 CFR 1045, http://www.gpoaccess.gov/CFR/index.html

3. Confidential Information

a. Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe; The lowest level of classification which consists of material which could be expected to cause some form of damage to national security.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and Executive Order 13292, "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

b. Except as may be expressly provided by statute, the use of the classification Confidential shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

Source: NARA. Eisenhower EO 10501, November 5, 1953 "Safeguarding Official Information in the Interests of the Defense of the United States." http://www.archives.gov/federal-register/executive-orders/1953-eisenhower.html

c. Confidential is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the appropriate official is able to identify or describe.

(ii) For RD and FRD, Confidential is applied to information, the unauthorized disclosure of which could reasonably be expected to cause undue risk to the common defense and security that the appropriate official is able to identify or describe.

Source: Energy. 10 CFR 1045, http://www.gpoaccess.gov/CFR/index.html

**Classification Markings | Control Markings** [31]
***See Classification / Security Classification***

[31] A uniform method of marking classified information is reflected in D.C.ID 1/7, which also called for a "control markings register" that lists all the markings authorized to classify a document. DoD. *Intelligence Community Classification and Control Markings Implementation*. See http://ww.fas.org/sgp/othergov/icmarkings.ppt

1. The physical act of indicating on classified material the assigned classification or change therein, together with such additional information as may be required to show authority for the classification or change and any special limitation on such material.

Source: "Preliminary Draft – Minimum Standards for the Handling and Transmission of Classified Information in Executive Departments and Agencies of the Federal Government. " Issued pursuant EO 9835, United States. Congress. House. Committee on Expenditures in the Executive Departments. Subcommittee on Extra Legal Activities in the Departments. *Investigation of Charges that Proposed Security Regulations Under Executive Order 9835 Will Limit Free Speech and a Free Press*: hearings before the United States House Committee on Expenditures in the Executive Departments, Subcommittee on Extra Legal Activities in the Departments, Eightieth Congress, first session, on Nov. 14, 1947. Y 4.Ex 7/13: Se 2; also see Harold Relyea. "Security Classified and Controlled Information: History, Status, and Emerging Management Issues." *CRS Report to Congress* June 26, 2006, http://www.fas.org/sgp/crs/secrecy/RL33494.pdf

2. Also referred to as **Dissemination Control Markings,** which identify the expansion or limitation on the distribution of information. Some Dissemination Controls are restricted to use by certain Agencies. The inclusion of these markings in the Register does not authorize use of these markings by other Agencies. Multiple entries may be chosen from this Dissemination Control category if applicable. If multiple entries are used, they are listed in the order in which they appear in the Register and the Implementation Manual. Use a comma with no space interjected as the separator between multiple Dissemination Control entries. Examples of control markings:

Authorized for Release To (REL)
Critical Nuclear Weapons Design Information (CNWDI)
For Official Use Only
Formerly Restricted Data (FRD)
IMCON (Controlled Imagery)
Not Releasable to Foreign Nationals (NOFORN)
Originator Controlled (ORCON)
Confidential (Caution) – Proprietary Information Involved (PROPIN)
Restricted Data (RD)
Risk Sensitive (RSEN)
SAMI (Sources and Methods Information)
Unclassified Controlled Nuclear Information (UCNI)

Source: U.S. Air Force. Memo "Implementation of New Classification Marking Requirements." May 30, 2006, http://www.fas.org/sgp/othergov/dod/af053006.pdf [good examples of portion markings].

3. The term "classification markings" comprises the following elements: classification level, classification category (if RD or FRD), caveats (special markings), classifier information, and originator identification. From this point forward, the term "classification markings" means the markings listed above. Any deviation from the standard classification markings will be stated specifically.

Other Markings. Markings other than classification markings are date of origin, classification of titles, unique identification numbers (accountable only), destruction date (TOP SECRET only), and portion marking (Originally classified NSI only).

Specific examples of markings, including their recommended use, format, and placement, are contained in DOE G 471.2-1, *Classified Matter Protection and Control Implementation Guide.*

Source: Department of Energy DOE M 471.2-1 "Manual for Classified Matter Protection and Control." September 26, 1995. http://fas.org/irp/doddir/doe/m471_2-1.htm and *DOE Marking Handbook: How to Mark Matter Containing Classified Information and Unclassified Controlled Information* September 29, 2006, http://www.pnl.gov/isrc/pdf/doe_marking_handbook_2006.pdf

4. Marking has six purposes:

a. Alert the holder that the item requires protection
b. Advise the holder of the level of protection
c. Show what is classified and what is not
d. Show how long the information requires protection
e. Give the information about the origin of the classification
f. Provide warnings about any special security requirements

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

5. **Nine Categories of Classification and Control Markings**:

U.S. Classification
Non-U.S. Classification
Joint Classification Markings
SCI Control System/Codeword
Special Access Requires
Foreign Government Information

Dissemination Controls
Non-Intelligence Community Markings
Declassification Date

Source: "DMS GENSER Message Security Classifications, Categories, and Marking Phrase Requirements," Defense Information Systems Agency, March 1999, http://www.fas.org/sgp/othergov/DoD/genser.pdf

6. The term classification markings comprises (contain) the following elements:

- Classification level
- Classification category (if Restricted Data or Formerly Restricted Data)
- Caveats (special markings)
- Originator identification

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

7. There are three essential markings required on all information as national security information (NSI). The following should appear on the face of each classified document, or will be applied to other classified media in the appropriate manner:

a. Classification Line at top and bottom
b. Portion Marking
c. Classification Block which consists of the following:

- identity, by name or personal identifier and position of the Original Classification Authority (OCA)
- The agency and office of origin
- Declassification instructions
- Reason for classification

Overall page marking is the highest level of classified information contained in or revealed on a page; Portion Marking means the application of certain classification markings to individual words, phrases, sentences, paragraphs, or sections of a
document to indicate their specific classification level and category (22 CFR 9 and 10 CFR 1045, respectively; see http://www.gpoaccess.gov/CFR/index.html)

**An excellent illustration of marking is here:**
http://www.fas.org/sgp/news/2005/08/usa0805.html

8. Authorized non-U.S. classification markings are

- Top Secret (TS)
- Secret (S)
- Confidential (C)
- Restricted (R)
- Unclassified (U)

and are used by countries and international organizations. Usually designated by a trigraph country code (example: DEU= Germany)

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf; also see chart "Classification and Control Markings Made Easy."

9. Policy guidelines for the classification, marking, and declassification of national security information are found in the President's Executive Order 12958, Classified National Security Information, April 17, 1995 (http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html; the DoD *Guide to Marking Classified Documents,* DoD 5200.1-PH, http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoD5200_1ph.pdf; Classification and marking guidelines for defense industry are in Chapter 4 of the *National Industrial Security Program Operating Manual*, http://www.dtic.mil/whs/directives/corres/html/522022m.htm

**Types of Markings:** [32]

- **25X**

1. This marking is applied to information when it has been exempted from 25-year old automatic declassification and cannot be used unless the specific information has been approved through the Interagency Security Classification Appeals Panel (ISCAP) process. When this marking is used, it appears on the "Declassify on" line plus a brief reference to the category(ies) in section of 3.3b of the (Executive) Order 12958, and the new date or event of declassification.

Source: Defense Intelligence Agency. Office of Security and Counterintelligence, Policy and Security Awareness Branch. *Desk Reference Guide to Executive Order 12958, as Amended, Classified National Security Information.* April 2004.

---

[32] For historical background on the development of classification see the preface to Arvin S. Quist's "Security Classification of Information" at Federation of American Scientists website, http://www.fas.org/sgp/library/quist/preface-rev.html

2. The "25X" markings other than "25X-1-human" are applied when information is exempt from 25-year automatic declassification, and cannot be used unless the specific information has been approved through the Interagency Security Classification Appeals Panel (ISCAP) generally in the form of a declassification guide.

Source: Information Security Oversight Office. Marking Classified National Security Information Booklet. ISOO Implementing Directive No. 1 Effective September 22, 2003, http://www.archives.gov/isoo/training/marking-booklet.pdf

- **25X-human**

The identity of a confidential human source or human intelligence source is not subject to automatic declassification. The marking for the exemption of this specific information is: Declassify on: 25X1-human. This 25X-1-human marking applies only to confidential human sources or human intelligence sources, not all intelligence sources and methods.

Source: Information Security Oversight Office. Marking Classified National Security Information Booklet. ISOO Implementing Directive No. 1 Effective September 22, 2003, http://www.archives.gov/isoo/training/marking-booklet.pdf

- **ATOMAL**

NATO marking for U.S./U.K atomic-related information. The ATOMAL category is either U.S. Restricted Data or Formerly Restricted Data or United Kingdom Atomic Information that has been officially released to NATO. Depending upon the damage that would result from unauthorized disclosure, ATOMAL information is classified either

- COSMIC TOP SECRET ATOMAL (CTSA)
- NATO SECRET ATOMAL(NSA)
- NATO CONFIDENTIAL ATOMAL (NCA)

Source: Department of Energy DOE M 471.2-1 "Manual for Classified Matter Protection and Control." September 26, 1995, http://fas.org/irp/doddir/doe/m471_2-1.htm

- **AUTHORIZED FOR RELEASE TO** (name of country(ies)/international organization)" (REL)

This marking is used to identify Intelligence Information that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign/international organization indicated. This marking may be abbreviated "REL (abbreviated name of foreign organization)."

Source: DoD. National Industrial Security Program Operating Manual (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

- **Background Use Only**

An obsolete control marking not used after the issuance of "Security Controls on the Dissemination of Intelligence Information," April 12, 1995.

Source: Revised D.C.ID 1/7, "Security Controls on the Dissemination of Intelligence Information." http://www.fas.org/irp/offdocs/D.C.id17.htm

- **Controlled Enhanced Safeguards**

Defined as measures more stringent than those normally required since inadvertent or unauthorized disclosure would create a risk of substantial harm.

Source: To accompany the Presidential Memorandum, Background on the Controlled Unclassified Information Framework, released May 9, 2008, http://www.fas.org/sgp/cui/background.pdf

- **Critical Nuclear Weapons Design Information (CNWDI)**

1. Department of Defense marking for Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and totally contained quantities of fissionable, fusionable, and high-explosive materials by type. Among these excluded items are the components which military personnel, including contractor personnel, set, maintain, operate, test, or replace.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. DoD category of weapons data that is comparable to "top secret" or "secret restricted data." Disseminated within the DOD on a need-to-know basis, it includes information relating to the theory of operation or design of the components of a nuclear weapon. CNWDI excludes a number of less sensitive information related to the maintenance and operation of nuclear weapons.

Source: Stephen Schwartz (ed.), *Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons Since 1940*. Brookings Institute. http://www.brook.edu/fp/projects/nucwcost/box8-1.htm and DoD. National Industrial Security Program Operating Manual (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

- **CRYPTO**

Marking or designator identifying COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government derived information.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, May 2003, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Director of Central Intelligence Authorized Control Markings | DCID 1/7 "Security Controls on the Dissemination of Intelligence Information"**

1. The four caveats approved for use with other security markings are:

ORCON. Dissemination and extraction of information controlled by Originator
PROPIN. Caution – Proprietary Information Involved.
NOFORN. Not Releasable to Foreign Nationals.
REL. (TO) Authorized Release To (countries/country).

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. Obsolete Restrictions and Control Markings | DCID 1/7

12.1 The following control markings are obsolete and will not be used in accordance with the following guidelines:

12.1.1 WNINTEL and NOCONTRACT. The control markings, Warning Notice – Intelligence Sources or Methods Involved (WNINTEL), and NOT RELEASABLE TO CONTRACTORS/CONSULTANTS (abbreviated NOCONTRACT or NC) **were rendered obsolete effective 12 April 1995**. No permission of the originator is required to release, in accordance with this Directive, material marked WNINTEL. Holders of documents prior to 12 April 1995 bearing the NOCONTRACT marking should apply the policies and procedures contained in Section 6.1 for possible release of such documents.

12.1.2 Remarking of material bearing the WNINTEL, or NOCONTRACT, control marking is not required; however, holders of material bearing these markings may line through or otherwise remove the marking(s) from documents or other material.

12.1.3 Other obsolete markings include: WARNING NOTICE INTELLIGENCE SOURCES OR METHODS INVOLVED, WARNING NOTICE SENSITIVE SOURCES AND METHODS INVOLVED,

WARNING NOTICE INTELLIGENCE SOURCES AND METHODS INVOLVED, WARNING NOTICE SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY, USIB ONLY, NFIB ONLY.

[I reported this 3 years ago – I wonder if anyone shipped a copy of DCID 1/7 over to State; see below, Department of State, Foreign Service Manual, 12FAM529.11, page 10, "Identification, Marking and Handling," http://foia.state.gov/masterdocs/12fam/12m0520.pdf ]

Source: Director of Central Intelligence "Directive 1/7 Security Controls on the Dissemination of Intelligence Information." June 30, 1998, http://www.fas.org/irp/offdocs/D.C.id1-7.html

- **Dissemination and Extraction of Information Controlled by Originator (ORCON)**

1. This marking may be used only on Intelligence Information that clearly identifies or would reasonably permit ready identification of an intelligence source or method that is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may be abbreviated as "ORCON" or "OC."

Source: DoD. National Industrial Security Program Operating Manual (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

- **Distribution Limitation**

Unclassified technical data with military or space application is marked with a distribution statement to limit data access to government agencies, DoD components, contractors, and those eligible for export-control data. A distribution statement marking is distinct from, and in addition to, a security and classification marking. Following is a brief description of the various statements:

**Statement "A".** Approved for public release; distribution is unlimited. Before a document can be marked Statement "A", it must be processed for public release through Public Affairs Security Review channels.

**Statement "B".** Distribution authorized to US Government agencies only.

**Statement "C".** Distribution authorized to US Government agencies and their contractors.

**Statement "D".** Distribution authorized to DoD and DoD contractors only.

**Statement "E".** Distribution to DoD components only.

**Statement "F".** Further dissemination only as directed by (insert controlling DoD office) (date of determination) or higher DoD authority. Normally used only on classified documents.

**Statement "X".** Distribution authorized to government agencies and private individuals or enterprises eligible to obtain export-controlled technical data.

Source: DoD. "Distribution Statements on Technical Documents," March 18, 1987, http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf

- **Drug Enforcement Administration Sensitive Information**

Unclassified documents containing DEA Sensitive information shall be marked "DEA Sensitive" at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).

b. In unclassified documents, each page containing DEA Sensitive information shall be marked "DEA Sensitive" top and bottom. Classified documents containing DEA Sensitive information shall be marked as required by Chapter 5, except that pages containing DEA Sensitive information but no classified information will be marked "DEA Sensitive" top and bottom.

c. Portions of DoD documents that contain DEA Sensitive information shall be marked "(DEA)" at the beginning of the portion. This applies to classified, as well as unclassified documents. If a portion of a classified document contains both classified and DEA Sensitive information, the "DEA" marking shall be included along with the parenthetical classification marking.

Source: DoD. DOD 5200.1-R. "Information Security Program." Appendix C. January 1997. http://fas.org/irp/doddir/dod/5200-1r/appendix_c.htm

- **Exclusive Distribution (EXDIS)**

Means distribution exclusively to officers with essential need-to-know. This caption is used only for highly sensitive traffic between the White House, the Secretary, the Under Secretaries, and chief of mission. Documents bearing this special distribution caption shall be treated as NOFORN. These documents must be given the physical protection prescribed by their classification.

Source: Department of State. Foreign Service Manual. 12 FAM 530 "Storing and Safeguarding Classified Material." http://www.state.gov/m/a/dir/regs/fam/

- **For Official Use Only (FOUO)**

1. Information that has been determined to qualify for FOUO status should be indicated by markings when included in documents and similar material. Markings should be applied at the

time documents are drafted, whenever possible, to promote proper protection of the information.

Unclassified documents and material containing FOUO information shall be marked as follows:

(1) Documents will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one).
(2) Pages of the document that contain FOUO information shall be marked "FOR OFFICIAL USE ONLY" at the bottom.
(3) Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings which alert the holder or viewer that the material contains FOUO information.
(4) FOUO documents and material transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

This document contains information exempt from mandatory disclosure under the FOIA.

Exemption(s) ____ apply.

Classified documents and material containing FOUO information shall be marked as required by Chapter V of this regulation, with FOUO information identified as follows:

(1) Overall markings on the document shall follow the rules in Chapter 5. No special markings are required on the face of the document because it contains FOUO information.
(2) Portions of the document shall be marked with their classification as required by Chapter 5. If there are unclassified portions that contain FOUO information, they shall be marked with "FOUO" in parentheses at the beginning of the portion. Since FOUO information is, by definition, unclassified, the "FOUO" is an acceptable substitute for the normal "U."
(3) Pages of the document that contain classified information shall be marked as required by Chapter 5. Pages that contain FOUO information but no classified information will be marked "FOR OFFICIAL USE ONLY" at the top and bottom.

Transmittal documents that have no classified material attached, but do have FOUO attachments shall be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT."

Each part of electrically transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text.

Source: DoD. DOD 5200.1-R "Information Security Program." Appendix C. January 1997, http://fas.org/irp/doddir/dod/5200-1r/appendix_c.htm

2. Both DOE and DOD base their programs on the premise that information designated as OUO or FOUO must (1) have the potential to cause foreseeable harm to governmental, commercial, or private interests if disseminated to the public or persons who do not need the information to perform their jobs and (2) fall under at least one of eight Freedom of Information Act (FOIA) exemptions. According to GAO's Standards for Internal Control in the Federal Government, policies, procedures, techniques, and mechanisms should be in place to manage agency activities. However, while DOE and DOD have policies in place, our analysis of these policies showed a lack of clarity in key areas that could allow for inconsistencies and errors. For example, it is unclear which DOD office is responsible for the FOUO program, and whether personnel designating a document as FOUO should note the FOIA exemption used as the basis for the designation on the document.

Source: General Accountability Office. "Managing Sensitive Information: Departments of Energy and Defense Policies and Oversight Could Be Improved." GAO-06-369, March 7, 2006, http://www.gao.gov/htext/d06369.html and "Managing Sensitive Information: DOE and DOD Could Improve Their Policies and Oversight: Statement of Davi M. D'Agostino." GAO-06-531T. March 14, 2006, http://www.gao.gov/htext/d06531t.html

3. The Department of Homeland Security report to Congress, marked "For Official Use Only" on the status of defenses against shoulder-fired anti-aircraft missiles was removed from the Federation of American Scientists web site after DHS objected to its publication. "If the Report is not removed from your website within 2 business days, we will consider further appropriate actions necessary to protect the information contained in the Report," Mr. Anderson wrote. See his August 9 letter here: http://www.fas.org/sgp/news/2006/08/dhs080906.pdf

Source: FAS. *Secrecy News* Issue 90, August 14, 2006, http://www.fas.org/sgp/news/secrecy/

- **Limited Dissemination**

1. Restrictive Controls for classified information established by an original classification authority to emphasize need-to-know measures available within the regular security system.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. Establishes measures for the protection of information beyond those involving access to classified information per se, but not so stringent as to require the establishment of a Special Access Program. It prohibits use of terminology indicating enhancements to need-to-know, such as Special Need-to-Know (SNTK), MUST KNOW, Controlled Need-to-Know (CNTK), Close Hold, or other similar security upgrade designations and associated unique security requirements such as specialized nondisclosure statements.

Source: John Pike. "Security and Classification." http://www.ostgate.com/classification.html

3. Used to identify unclassified geospatial information and data which the SecDEF may withhold from public disclosure; may only be used with UNCLASSIFIED.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

4. Means distribution strictly limited to officers, offices, and agencies with need-to-know. This caption is reserved for messages of more than usual sensitivity. Material captioned "LIMDIS" is to be controlled, handled, and stored in accordance with the classification level of the information involved.

Source: Department of State. Foreign Service Manual. 12 FAM 530 "Storing and Safeguarding Classified Material." http://www.state.gov/m/a/dir/regs/fam/

- **NATO UNCLASSIFIED**

This marking is applied to NATO information that does not require security protection, and is handled in accordance with information management procedures.

Source: Department of Energy DOE M 471.2-1 "Manual for Classified Matter Protection and Control." September 26, 1995, http://fas.org/irp/doddir/doe/m471_2-1.htm

- **No Distribution**

Means no distribution to other than addressee without the approval of the Executive Secretary. This caption is used only on messages of the highest sensitivity between the President, the Secretary of State, and chiefs of mission. Documents bearing this special distribution caption shall be treated as NOFORN. These documents must be given the physical protection prescribed by their classification.

Source: Department of State. Foreign Service Manual. 12 FAM 530 "Storing and Safeguarding Classified Material." http://www.state.gov/m/a/dir/regs/fam/

- **Non-Intelligence Community Markings**

Communications Security Material (COMSEC)
Protective measure to prevent unauthorized persons from receiving classified information via telecommunications.

May be used with Top Secret, Secret, Confidential or Unclassified.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

- **NOT RELEASABLE TO CONTRACTORS/CONSULTANTS (NOCONTRACT or NC)**

This marking may be used only on Intelligence Information that is provided by a source on the express or implied condition that it not be made available to contractors; or that, if disclosed to a contractor, would actually or potentially give him/her a competitive advantage, which could reasonably be expected to cause a conflict of interest with his/her obligation to protect the information. This marking may be abbreviated as "NOCONTRACT" or "NC."

Source: DoD. *National Industrial Security Program Operating Manual* (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

- **NOT RELEASABLE TO FOREIGN NATIONALS**

  This marking is used to identify Intelligence Information that may not be released in any form to foreign governments, foreign nationals, or non-U.S. citizens. This marking may be abbreviated "NOFORN" or "NF."

Source: DoD. *National Industrial Security Program Operating Manual* (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

- **Official Use Only**

A security classification marking used during the period July 18, 1949 through October 22, 1951.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

- **Originating Agency's Determination Required**

  1. Indicates that the information must be reviewed by the originator before any declassification can take place.

Source: NISPOM. Chapter 4. "Classification and Marking."
http://www.fas.org/sgp/library/nispom/chap_04.htm

2. "OADR" is not an approved marking for documents originally classified under E.O. 12958, as amended, and should not be contained in any originally classified documents that have been created after October 14, 1995.

Source: Information Security Oversight Office. Marking Classified National Security Information Booklet. ISOO Implementing Directive No. 1 Effective September 22, 2003,
http://www.archives.gov/isoo/training/marking-booklet.pdf

- **Portion Markings**

1. Every portion (normally paragraphs, but also including subjects, titles, charts, etc.) shall be portion marked to indicate which portions are classified, and at what level, and which portions are unclassified. Portion markings shall always be placed at the beginning of the portions. The symbols TS (Top Secret), S (Secret), C (Confidential) and U (Unclassified) are used to indicate the classification level.

Source: Defense Intelligence Agency. Office of Security and Counterintelligence, Policy and Security Awareness Branch. *Desk Reference Guide to Executive Order 12958, as Amended, Classified National Security Information.* April 2004.

2. A portion is ordinarily defined as a paragraph, but also includes charts, tables, pictures, and illustrations, as well as subjects and titles. Portion markings consist of the letters "(U)" for unclassified, "(C)" for "Confidential," "(S)" for "Secret," and "(TS)" for "Top Secret." These abbreviations, in parentheses, are placed before or after the portion to which they apply.

Source: Information Security Oversight Office. Marking Classified National Security Information Booklet. ISOO Implementing Directive No. 1 Effective September 22, 2003,
http://www.archives.gov/isoo/training/marking-booklet.pdf

- **Caution – (Confidential) Proprietary Information Involved (PROPIN)**

This marking is used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a trade secret or proprietary data believed to have actual or

potential value. This marking may be used in conjunction with the "NOCONTRACT" marking to preclude dissemination to any contractor. This marking may be abbreviated as "PROPIN" or "PR."

Source: DoD. *National Industrial Security Program Operating Manual* (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

- **(Protected) Critical Infrastructure Information**

The Protected CII Program Manager or the Protected CII Program Manager's designees shall mark Protected CII materials as follows: "This document contains Protected CII. In accordance with the provisions of 6 CFR part 29, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b) (3)). Unauthorized release may result in civil penalty or other action. It is to be safeguarded and disseminated in accordance with Protected CII Program requirements."

Source: Department of Homeland Security. "Protected Critical Infrastructure Information." 6 CFR 29.6, http://www.gpoaccess.gov/cfr/index.html

- **Releasable by Information Disclosure Official (RELIDO)**

Effective immediately, the Intelligence Community may use the dissemination marking Releasable By Information Disclosure Official (RELIDO) to facilitate information sharing through streamlined, rapid release decisions by authorized disclosure officials. RELIDO is a dissemination marking that may be applied to intelligence information to indicate that the originator has authorized Designated Intelligence Disclosure Officials (DIDO) to make further sharing decisions in accordance with the existing procedures for uncaveated intelligence material (intelligence with no restrictive dissemination controls). RELIDO may be used independently or in conjunction with the "REL TO" dissemination marking. When the RELIDO marking is applied by the originator, the releasing DIDO must follow existing sharing guidelines and maintain accurate records of all sharing decisions consistent with D.C.I directives. RELIDO will be incorporated into the Authorized Classification and Control Markings Register maintained by the Controlled Access Program Coordination Office (CAPCO) in accordance with D.C.ID 6/6 IX H.

Source: Director of Central Intelligence Directive. "Intelligence Community Implementation of Releasable by Information Disclosure Official (RELIDO) Dissemination Marking." DCID 8 Series Policy Memoranda 1, June 9, 2005, http://www.fas.org/irp/offdocs/D.C.id8-memo.html

- **REL TO**

REL TO identifies information that an originator has predetermined to be releasable or has been released, through established foreign disclosure procedures and channels, to the foreign

country indicated. REL TO must include country code "USA" as the first country code listed for U.S. classified information. Other countries follow in alphabetical order with each country code separated by a comma and a space with the last country code separated by a space, a lower case "and", and a space.

Source: DoD. "Intelligence Community Classification and Control Markings Implementation." http://www.fas.org/sgp/othergov/icmarkings.ppt

- **Restricted**

An active security classification marking used by some foreign governments and international organizations.

Eisenhower EO 10501, November 5, 1953 "Safeguarding Official Information in the Interests of the Defense of the United States" eliminated the "Restricted" level leaving only Top Secret, Secret, and Confidential. Made a differentiation between national security and national defense.

Source: National Archives and Records Administration (NARA). http://www.archives.gov/federal-register/executive-orders/1953-eisenhower.html and Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

- **Sensitive But Unclassified**

Information that has been **determined** to be SBU should be designated as "Sensitive But Unclassified" with the appropriate markings and labels.

Source: Centers for Disease Control. "Manual Guide - Information Security CD.C.-02."
Office of Security and Emergency Preparedness "Sensitive But Unclassified Information." Part B. 07/22/2005, http://www.fas.org/sgp/othergov/cD.C.-sbu.pdf

- **State Distribution Only**

Precludes initial distribution to other federal agencies and is used when disclosure of certain communications to other agencies would be prejudicial to the best interests of the Department of State. This caption may be used in conjunction with the captions "EXDIS" and LIMDIS." Material captioned "STADIS" is to be controlled, handled, and stored in accordance with the classification level of the information involved.

Source: Department of State. *Foreign Service Manual*. 12 FAM 530 "Storing and Safeguarding Classified Material." http://www.state.gov/m/a/dir/regs/fam/

- **Unclassified Information**

1. Information, a document, or material that has been determined not to be classified or that has been declassified by a proper authority; Also defined as a limited distribution category applied to the wide range of unclassified types of official information, not requiring protection as National Security Information, but limited to official use and not publicly releasable.

Other similar markings, such as **For Official Use Only** (FOUO) and **Limited Official Use** are not used to identify classified information, and along with other term such as **Sensitive, Conference, or Agency,** are used as **distribution markings**, and are not authorized classification designations to identify classified information.

Under an 18 October 1983 memorandum, six distribution statements, designated A through F, were approved establishing categories of Unclassified/Limited Data:

A. **Approved for Public Release** Documents are available to the public, foreign nationals, companies, foreign governments, and may be exported without a license.

B. **Limited to Government Agencies Information** covers weapons test and evaluation data, contractor performance evaluation records, foreign government data and proprietary information.

C. **Limited to Government Agencies and their Contractors** includes documents involving critical technologies that advance the state of the art in an area of significant or potentially significant military application.

D. **Limited to DOD and DOD Contractors Only** is designed to protect information on system or hardware in the development of concept stage, which must be protected to prevent premature dissemination.

E. **Distribution to DOD Components Only**

F. **Further Dissemination Only As Directed** is normally imposed only on classified documents, but may be used on unclassified documents where specific authority exists.

Source: John Pike. "Security and Classification." http://www.ostgate.com/classification.html

2. Distribution authorized to US Government agencies only (B, "Distribution authorized to US Government agencies only "above):

Source: Steven D. Pomper. *Asymmetric: Myth in United States Military Doctrine*. Thesis. Durham, NH: University of New Hampshire, 1991. 36-37. ADA428994
http://www.dtic.mil/matris/t-docs/TRAIL_MPT_2-22-05.html

- **Warning Notice-Intelligence Sources or Methods Involved (WNINTEL)**

This marking is used only on Intelligence Information that identifies or would reasonably permit identification of an intelligence source or method that is susceptible to countermeasures that could nullify or reduce its effectiveness. This marking may be abbreviated as "WNINTEL" or "WN." This marking may not be used in conjunction with special access or sensitive compartmented information (SCI) controls.

Source: DoD. *National Industrial Security Program Operating Manual* (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

- **Warning Notices**

Warning notices sometimes appear on classified documents to alert the reader that special precautions are required in the handling and releasing of information. When required, the warning notices defined below shall appear in their full form on the front cover, title page, or first page of a document. The short form shall appear at the top or bottom center of applicable pages, on telegram caption lines, and on tables, figures, charts, etc. The abbreviated form is used following the classification symbol in portion marking.

When dissemination of information is restricted to appropriately cleared U.S. citizens, use the following notice: [short form/abbreviated form]:

**NOT RELEASABLE TO FOREIGN NATIONALS NOFORN/NF**

When information is limited only to U.S. Government employees, use the following notice:

**NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR CONSULTANTS NO CONTRACT/NC**

When information has been provided to the United States by foreign government or international organization, or information is generated by the United States pursuant to a joint arrangement with foreign government or international organization, use the notice:

**FOREIGN GOVERNMENT INFORMATION/FGI**

If the information is foreign government information that must be concealed, do not use the marking and mark the document as if it were entirely of U.S. origin. If the marking is deleted, the originator must maintain a record of the source of the information.

When information identifies or would reasonably permit identification of an intelligence source or method that is susceptible to countermeasures that could nullify or reduce its effectiveness,

use the following notice:

**WARNING NOTICE - INTELLIGENCE SOURCES OR METHODS INVOLVED**
**WNINTEL/WN**
When the originator must have continuing knowledge and supervision of the use of information, use the following notice:

**DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR**
**ORCON/OC**
For classified material containing Restricted Data or Formerly Restricted Data, as defined by the Atomic Energy Act of 1954 as amended (which concerns the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy), the markings prescribed by the Department of Energy will be applied as follows:

RESTRICTED DATA. THIS MATERIAL CONTAINS RESTRICTED DATA AS DEFINED IN THE ATOMIC ENERGY ACT OF 1954. UNAUTHORIZED DISCLOSURE SUBJECT TO ADMINISTRATIVE AND CRIMINAL SANCTIONS RESTRICTED DATA /RD or

FORMERLY RESTRICTED DATA. UNAUTHORIZED DISCLOSURE SUBJECT TO ADMINISTRATIVE AND CRIMINAL SANCTIONS. HANDLE AS RESTRICTED DATA IN FOREIGN DISSEMINATION. SECTION 144B, ATOMIC ENERGY ACT OF 1954 FORMERLY RESTRICTED DATA/FRD

Before release to contractors, communication security (COMSEC) documents will be annotated on the title page or first page as follows:

COMSEC MATERIAL - ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE

Place this notation on COMSEC documents at the time of their origination when release to contractors is anticipated. A.I.D. COMSEC material will be marked in accordance with Communications Security Policy, CSP 1. Foreign dissemination of COMSEC information is governed by NCSC Policy Directive 6.

Source: Department of State. *Foreign Service Manual*. 12FAM529.11 "Identification, Marking and Handling." http://www.state.gov/m/a/dir/regs/fam/

- **X1 through X8**

X1-X8 are not approved markings for documents originally classified under E.0. 12958 as amended, and should not be contained in any originally classified documents on, or after, September 22, 2003.

Source: Information Security Oversight Office. Marking Classified National Security Information Booklet. ISOO Implementing Directive No.1 Effective September 22, 2003, http://www.archives.gov/isoo/training/marking-booklet.pdf

10. Because security classification, however, was not possible for some kinds of information deemed in some quarters to be "sensitive," other kinds of designations or markings came to be applied to alert federal employees regarding its privileged or potentially harmful character. Sometimes these markings derived from statutory provisions requiring the protection of a type of information, others were administratively authorized with little detail about their use.

Source: Harold C. Relyea, "Security Classified and Controlled Information: History, Status, and Emerging Management Issues. *CRS Report to Congress* RL 33494, updated February 11, 2008, http://www.opencrs.com

**Note:** On May 12, 2008, Director of National Intelligence released "Authorized Classification and Control Markings Register," http:/tinyurl.com/ye7yqxr,"

This system uses a uniform list of security classification and control markings authorized for all dissemination of classified national intelligence information by components of the IC. This marking system augments and further defines the markings requirements established in Executive Order 12958, as amended, for portion markings and overall classification. This system does not stipulate or modify the classification authority information required by E.O. 12958, as amended.

(U) Purpose
(U) This Authorized Classification and Control Markings Register is maintained by the Controlled Access Program Coordination Office (CAPCO) (hereafter, referred to as the CAPCO Register…

Based on this information, this section of the *Lexicon* will be maintained.

## Classification Priesthood

National classification elite is a kind of secret society, closed to the uninitiated. It is a sect marked by a rigorous internal discipline, highly developed rituals, a strict hierarchy, and a consistent philosophy. Central to this philosophy is the principle of compartmentalization, which holds that the best way to control of information is to break it into little pieces, and never to allow too much to be assembled in one place.

The classification priesthood has developed an elaborate system to protect its secrets. The priesthood makes a distinction between classifying documents and classifying the information contained within them.

Source: Stephen Hilgartner, Richard C. Bell, and Rory O'Connor.*Nukespeak.* New York: Penguin Books, 1982. 58-59.

### Classified At Birth

***See Born Classified*, *Nuclear Secrecy***

Based on the "born secret" interpretation of the Atomic Energy Act of 1954 wherein a "writer or researcher could working from unclassified sources could combine information in such a way as to produce concepts that are 'classified at birth'." DeVolpi et al (12) state that the inclusion of privately generated information under classification authority derived from Carter EO 12065 or the Atomic Energy Act is "far from clear."

DOE asserts that all information which falls under Restricted Data "comes into existence as classified."

Source: Atomic Energy Act of 1954 (P.L. 83-703), Alexander DeVolpi et al. *Born Secret: the H-bomb, the Progressive Case and National Security.* New York: Pergamon Press, 1981, and Howard Morland. "The Holocaust Bomb: a Question of Time." FAS e-Prints, http://www.fas.org/sgp/eprint/morland.html

### Classified Community

An often-invoked but ill defined entity that in this case [describing Project Sherwood] is comprised of secret conferences, publications, and interlocking advisory committees… classified communities, a key Cold War invention provided a kind of ersatz scientific openness. The combination of classified conferences and publications fostered a free flow of information among the national labs. Because most lab scientists held clearances and hence could plug into this network, there was little chance of missing relevant research or review.

Source: Peter Westwick. "In the Beginning." *Bulletin of Atomic Scientists*. November-December, 2000, http://www.thebulletin.org/article.php?art_ofn=nd00westwick

### Classified Defense Information

***See* Classification*, Classification Markings* / *Control Markings***

Defense information which is classified Top Secret, Secret, or Confidential, depending on the sensitivity of the information.

Source: Department of the Army Dictionary *of United States Army Terms*. Army Regulation 310-25. October, 1983,http://www.fas.org/irp/doddir/army/ar310-25.pdf

**Classified Information**

***See Classified Information Procedures Act***

1. "Classified national security information" or "classified information" means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended, http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2

2. (A) any information or material that has been determined by an official of the United States pursuant to law, an Executive Order, or regulation to require protection against unauthorized disclosure for reasons of national security, and

(B) any restricted data, as defined in section 11(y) of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)

Source: 10 U.S.C. 47 § 801, http://www.gpoaccess.gov/uscode/browse.html

3. Any information or material that has been determined by the United States Government, pursuant to an executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r or section 11 of the Atomic Energy Act of 1954. [42 U.S.C. 2014(y)]

Source: Public Law (PL) 96-456, Classified Information Procedures Act, Department of Justice. "Synopsis of CIPA." http://tinyurl.com/yc4flmy

4. DOE's strategy for protecting and controlling classified documents at DOE facilities involves a "graded protection system. Under such a system, the level of protection for a classified document is commensurate with the threat to the document, the vulnerability of the document, the value of the document, and the level of risk to the document that DOE is willing to accept. Not all items are protected to the same degree.

Source: *Nuclear Security: Information on DOE's Requirements for Protecting and Controlling Classified Documents* : statement of Jim Wells, Director, Energy, Resources, and Science Issues, Resources, Community, and Economic Development Division, before the Subcommittee on Oversight and

Investigations, Committee on Commerce, House of Representatives. Washington, D.C.: U.S. General Accounting Office, 2000. GAO/T-RCED-00 247, http://www.gao.gov/

5. A person not entitled to receive classified information until after he or she has received a security briefing covering the provisions of this regulation and has executed a non disclosure agreement (Form SF-312) according to National Security Decision Directive 84 (NSDD 84) dated March 11, 1983.

Source: U.S. Department of State *Foreign Affairs Manual*. "Storing and Safeguarding Classified Material." 12 FAM 530. (12 FAM 536.1-4 "Determination of Security Briefing"), http://www.state.gov/m/a/dir/regs/fam/

**Classified Information Procedures Act (CIPA) PL 96-456**
***See Graymail***

1. Among other things, CIPA allows a court to "upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the *Federal Rules of Criminal Procedure,* to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove." Sec. 4. "Discovery of classified information by defendants" states:

> The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the *Federal Rules of Criminal Procedure*, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove.

Source: 18 U.S.C. http://www.gpoaccess.gov/uscode/browse.html and Department of Justice. "Synopsis of CIPA." http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm02054.htm

**Classified Matter**
Official information or matter in any form or of any nature which requires protection in the interests of national security.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Classified Military Information (CMI)**
***See Classification***

Information which is originated by or for the DoD or its Components or is under their jurisdiction or control and which requires protection in the interests of national security. It is designated TOP SECRET, SECRET and CONFIDENTIAL as described in EO 12356. Classified military information may be disclosed in oral, visual or material form and is divided into eight categories:

a. Category 1 - Organization, Training And Employment Of Military Forces; b. Category 2 - Military Materiel And Munitions; c. Category 3 - Applied Research And Development Information; d. Category 4 - Production Information. Designs, drawings, chemical and mathematical equations, specifications, models, manufacturing techniques, software source code and related information (excluding Category 2 and 3 information) necessary to manufacture or substantially upgrade military materiel and munitions. The following information is furnished to further clarify the definition of Production Information:

(1) Manufacturing information
(2) Build-to-Print
(3) Assembly Information

e. Category 5 - Combined Military Operations, Planning And Readiness; f. Category 6 - U.S. Order Of Battle ; g. Category 7 - North American Defense; h. Category 8 - Military Intelligence

Source: DoD. *International Programs Security Handbook*. Chapter 3. Office of the Deputy to the Under Secretary of Defense (Policy) for Policy Support, 1993, http://www.fas.org/sgp/library/ipshbook/Chap_03.html and Army Regulation 380-10, "Foreign Disclosure and Contacts with Foreign Representatives," June 22, 2005, http://www.fas.org/irp/DoDdir/army/ar380-10.pdf

### Classified National Security Information

1. (c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Source: EO 12958, "Classified National Security Information, Amended," (April 17, 1995), http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html ; *The Nat'l Security. Archive Fund, Inc. v. CIA*, 402 F. Supp. 2d 211 (D.D.C. 2005), http://www.justice.gov/oip/attachmentedec98.htm

2. Sec. 2001.23 Additional requirements [1.6].
(a) Marking prohibitions. Markings other than "Top Secret," "Secret," and "Confidential," such as "For Official Use Only," "Sensitive But Unclassified," "Limited Official Use," or "Sensitive Security

Information" shall not be used to identify classified national security information. No other term or phrase shall be used in conjunction with these markings, such as "Secret Sensitive" or "Agency Confidential," to identify classified national security information. The terms "Top Secret," "Secret," and "Confidential" should not be used to identify non-classified executive branch information.

Source: ISOO and NARA, Classified National Security Information Directive No. 1, September 23, 2003, http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-directive.html#2001.15

### Classified Naval Nuclear Propulsion Information (C-NNPI)

All classified information concerning the design, arrangement development, manufacture, testing, operation, administration, training, maintenance, and repair of propulsion plants of naval nuclear powered ships and prototypes, including associated shipboard and shore-based nuclear support facilities.

Source: GAO. *Managing Sensitive Information: Actions Needed to Ensure Recent Changes in DOE Oversight Do Not Weaken an Effective Classification System*. June 26, 2006, http://www.gao.gov/new.items/d06785.pdf

### Classified NSA/CSS Information

***See Classification, Classified Information***

Information that is classified pursuant to the standards of Executive Order 12958, as amended, or any predecessor order. It includes, but is not limited to, intelligence and intelligence-related information, sensitive compartmented information (information concerning or derived from intelligence sources and methods), and cryptologic information (information concerning communications security and signals intelligence, including information which is also sensitive compartmented information) protected by Section 798 of Title 18, United States Code.

Source: NSA/CSS. "Reporting Unauthorized Media Disclosures of Classified NSA/CSS Information." NSA/CSS Policy 1-27, 20 March 2006, http://www.fas.org/irp/nsa/unauthorized.html

### Classifier

An individual who makes a classification determination and **applies** a security classification to information or material. A classifier may either be a classification authority or may assign a security classification based on a properly classified source or a classification guide.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/fam/

### Closed Information

Information that will either never be made public, or will become known decades after a particular action or event. Closed information is associated with "the right of an individual to see or use a particular type or level of classified information which is dependent on a need to see or know" (Cohen 2); Information that is compartmented, and therefore not available to the public, and cannot be accessed except by those who hold special access clearances. Closed information is associated with a specific level of privilege.

Source: Susan L. Maret; Sheldon Cohen. "Security Clearances and the Protection of National Security Information Law and Procedures." Defense Personnel Security Research Center, (DTIC) Technical Report 00-4. November, 2000. AD-A388100/NA, http://www.sheldoncohen.com/publications/security-clearances.htm

## Closed World

First air defenses, then strategic early warning and nuclear response, and later the sophisticated tactical systems of the electronic battlefield grew from the control and communications capacities of information machines. As metaphors, such systems constituted a dome of global technological oversight, a *closed world*, within which every event was interpreted as part of a titanic struggle between the superpowers. Inaugurated in the Truman Doctrine of "containment," elaborated in Rand Corporation theories of nuclear strategy, tested under fire in the jungles of Vietnam, and resurrected in the impenetrable "peace shield" of Ronald Reagan's Strategic Defense Initiative, the key theme of closed-world discourse was global surveillance and control through high-technology military power. Computers made the closed world work simultaneously as technology, as political system, and as ideological mirage.

Both the engineering and the politics of closed-world discourse centered around problems of *human-machine integration*: building weapons, systems, and strategies whose human and machine components could function as a seamless web, even on the global scales and in the vastly compressed time frames of superpower nuclear war. As symbol-manipulating logic machines, computers would automate or assist tasks of perception, reasoning, and control in integrated systems. Such goals, first accomplished in World War II-era anti-aircraft weapons, helped form both cybernetics, the grand theory of information and control in biological and mechanical systems, and artificial intelligence (AI), software that simulated complex symbolic thought. (1).

Source: Paul N. Edwards. *Closed World: Computers and the Politics of Discourse in Cold War America.* Cambridge, MA: MIT Press, 1996.

## Code

1. Any system of communication in which arbitrary groups of symbols represent units of plain text of varying length. Codes may be used for brevity or for security.

2. A cryptosystem in which the cryptographic equivalents (usually called "code groups"), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plain text elements which are primarily words, phrases, or sentences.

Source: DoD. *The Department of Defense Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Code Name | Codename** [33]

***See Codeword / Code Word, Exercise Term, NICKA, Nickname***

1. British and US jargon, aka code name. It has been used interchangeably with codeword in the past. Both codenames and nicknames were and are used in conjunction with operations and projects, whereas codewords and cryptonyms are used standing alone with a digraph prefix (Central Intelligence Agency (CIA) usage). Code names and nicknames are always the second part of an operation, plan or project title. N.B. As noted elsewhere, code words [and also codenames] are always classified; nicknames are always unclassified and consist of two separate words, e.g., BLUE BIRD is a nickname, but BLUEBIRD is a codeword or codename. Code names can be in military usage, either strategic or tactical. The former can be viable for years, unless compromised, while the latter are ephemeral.

Additionally, it should be noted that codenames are used in conjunction with military operations, operational or contingency plans, or concepts, whereas military projects are usually nonoperational intelligence, and counterintelligence usage may differ from military practice. Codewords can stand alone, and when used in codeword intelligence, they may or may not designate intelligence operations, but are otherwise used for access to the product of such operations.

Source: Leo D. Carl. *International Dictionary of Intelligence*. McLean, VA: International Defense Consultant Services, Inc., 1990.

2. Arkin writes there are three types of Code Names:
Nicknames | Code Words | Exercise Terms

For a detailed list of Codenames by country, see *Code Names: Deciphering US Military Plans, Programs, and Operations in the 9/11 World.*

Source: William M. Arkin. *Code Names: Deciphering US Military Plans, Programs, and Operations in the 9/11 World.* Hanover, NH: Steerforth Press, 2005, and his "Code Name of the Week" feature at the *Washington Post* http://blog.washingtonpost.com/earlywarning/code_name_of_the_week/

[33] I could not locate an official DoD definition for "code name." DoD employs the term "code word."

3. The American military adopted code names during the World War II era, primarily for security reasons. Its use of code names for operations grew out of the practice of color-coding war plans during the interwar period. Even before America entered the war, the War Department had executed Operation Indigo, the reinforcement of Iceland, and had dubbed plans to occupy the Azores and Dakar as Operations Gray and Black respectively.

Source: Gregory C. Sieminski. "The Art of Naming Operations." *Parameters: US Army War College Quarterly* Autumn 1995. [See the Wayback Machine,http://tinyurl.com/75guht ]

4. Code names are/were also used by the FBI. See Athan Theoharis, ed. *The FBI: A Comprehensive Reference Guide* (Phoenix: Oryx Press, 1998) for a number of code names used by the FBI since the J. Edgar Hoover days.

**Codeword | Code Word**

***See Code Names, Nicknames, Sensitive Compartmented Information (SCI), Sensitive Compartmented Information (SCI) Control Systems/Codewords***

1. Any series of designated words or terms used with a security classification to indicate that the material classified was derived through a sensitive source or method, constitutes a particular type of sensitive compartmentalized information (SCI), and is therefore accorded limited distribution.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

2. A single classified word assigned to represent a specific special access program; a unique name assigned to a project, program, or element of information for the purpose of safeguarding the true nature of the protected interest. Code words may consist of symbols, letters, or numbers, but do not include nicknames, chemical symbols or abbreviations.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

3. Designed to provide special protection, beyond that provided by the federal classification system, to a specific category of sensitive information; authorized by Section 9 of Executive Order 11652 (SEC. 9. "Special Departmental Arrangements: The originating Department or other appropriate authority may impose, in conformity with the provisions of this order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography.")

Source: Central Intelligence Agency. Center for the Study of Intelligence. "Critique of the Codeword Compartment of the CIA." March 1977, http://www.fas.org/sgp/othergov/codeword.html and EO 11652, March 8, 1972, http://www.fas.org/irp/offdocs/eo/eo-11652.htm.

4. A word that has been assigned a classification and a classified meaning to safeguard intentions and information regarding a classified plan or operation. b. A cryptonym used to identify sensitive intelligence data.

Source: DoD. *The Department of Defense Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

5. A single word from JANAP 299(S) which has an assigned classified meaning to secure and safeguard its information about actual real-world military plans or operations classified as CONFIDENTIAL or higher. Code words are not assigned from JANAP to test, drill, or exercise activities. A code word is placed in one of three categories:

(1) Available. Allocated to the using command. Available code words individually will be unclassified until placed in the active category; (2) Active. These are current and are assigned a classified meaning; (3) Canceled. Formerly active, but discontinued due to compromise, suspected compromise, cessation, or completion of the operation to which it pertained. Each canceled code word will not be used for 2 years and remains canceled until returned to the active category.

Source: HQ North American Aerospace Defense Command NORAD Regulation 11-3. Peterson Air Force Base, Colorado 80914-5002 25, August 1989. "Code Words, Nicknames and Exercise Terms." http://www.fas.org/spp/military/docops/norad/reg11003.htm and Chairman of the Joint Chiefs of Staff Manual. *Code Word, Nickname and Exercise Term Report (Short Title - NICKA)* April 1998, http://fas.org/irp/doddir/dod/cjcsm3150_29a.pdf

6. B. A code word is a single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified as CONFIDENTIAL or higher once activated.

Source: Department of the Navy, "Code Word, Nicknames, and Exercise Terminology System," OPNAVINST 5511.37D, January 30, 2007, http://www.fas.org/irp/doddir/navy/opnavinst/5511_37d.pdf

**Codeword Compartment**

Security device is designed to provide special protection, beyond that provided by the federal classification system, to a specific category of sensitive information.

Source: Central Intelligence Agency. Center for the Study of Intelligence. "Critique of the Codeword Compartment of the CIA." March 1977, http://www.fas.org/sgp/othergov/codeword.html

**Cognizant Security Agency (CSA)**

Agencies of the Executive Branch that have been authorized by reference (a) to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are: The Department of Defense, DOE, CIA, and NRC.

Source: DoD. National Industrial Security Manual (NISPOM). DoD 5220.22-M, February 28, 2006, https://www.dss.mil/GW/ShowBinary/DSS/isp/fac_clear/download_nispom.html

**Collateral Information**

***See Classification***

1. All national security information classified CONFIDENTIAL, SECRET AND TOP SECRET, under the provisions of an Executive Order for which special Intelligence Community. systems of compartmentation (such as sensitive compartmented information) are not formally established.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

2. Arkin describes Collateral Information as:

- Nonsensitive noncompartmentalized information classified Confidential, Secret or Top Secret.
- Sensitive Compartmentalized Information (SCI)
- Special intelligence (SI) a classified category of SI referring to signals

Source: William M. Arkin. *Code Names: Deciphering US Military Plans, Programs, and Operations in the 9/11 World.* Hanover, NH: Steerforth Press, 2005, and http://www.codenames.org/

**Collecting**

An activity of information management: the continuous acquisition of relevant information by any means, including direct observation, other organic resources, or other official, unofficial, or public sources from the information environment.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545-b.htm

**Collection**

1. The exploitation of sources by collection agencies, and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. Also, obtaining information or intelligence information in any manner, including direct observations, liaison with official agencies, or solicitation from official, unofficial, or public sources, or quantitative data from the test or operation of foreign systems.

Source: Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Springfield, VA: National Technical Information Service, [1999?]. SUDOC: PREX 3.2: C 76 and PREX 3.2/2: G 94

2. Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

Source: DoD 5240.1-R "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons." December, 1982, http://www.fas.org/irp/doddir/dod/d5240_1_r.pdf

**Collection Agency**

Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. See also agency.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Collection Management**

In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Collection of Information**

1. 7 (A) means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either--

(i) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the United States; or

(ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes; and

(B) shall not include a collection of information described under section 3518(c) (1) of title 44, United States Code.

Source: "The Analysis of Regulatory Functions." 5 U.S.C. 601, http://www.gpoaccess.gov/uscode/browse.html

2. Collection of information means, except as provided in Sec. 1320.4, the obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of information by or for an agency by means of identical questions posed to, or identical reporting, recordkeeping, or disclosure requirements imposed on, ten or more persons, whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit.

Collection of information includes any requirement or request for persons to obtain, maintain, retain, report, or publicly disclose information. As used in this Part, "collection of information" refers to the act of collecting or disclosing information, to the information to be collected or disclosed, to a plan and/or an instrument calling for the collection or disclosure of information, or any of these, as appropriate.

(1)A "collection of information" may be in any form or format, including the use of report forms; application forms; schedules; questionnaires; surveys; reporting or recordkeeping requirements; contracts; agreements; policy statements; plans; rules or regulations; planning requirements; circulars; directives; instructions; bulletins;
requests for proposal or other procurement requirements; interview guides; oral communications; posting, notification, labeling, or similar disclosure requirements; telegraphic or telephonic requests; automated, electronic, mechanical, or other technological collection techniques; standard questionnaires used to monitor compliance with agency requirements; or any other techniques or technological methods used to monitor compliance with agency requirements. A "collection of information" may implicitly or explicitly include related collection of information requirements.

Source. Office of Management and Budget. 5 CFR 1320. "Controlling Paperwork Burdens on the Public." http://www.gpoaccess.gov/cfr/index.html

### Collection Plan

A DoD and NATO term for a plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. [Note: the Army term is "intelligence, surveillance, and reconnaissance (ISR) plan."]

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545-b.htm

### Combat Information

***See Information***

Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545-b.htm

### Combat Zones That See

***See Urban Resolve 2015***

The inherently three-dimensional nature of urban centers, with large buildings, extensive underground passageways, and concealment from above requires the use of close-in imagery sensing, to obtain vital reconnaissance and targeting information. The rapid proliferation of low-cost video sensors presents an opportunity to obtain the necessary reconnaissance and targeting information by deploying large numbers of video cameras. The key technical goal of Combat Zones That See is to produce the algorithms for automatically monitoring video feeds to provide the reconnaissance and targeting information needed 24/7 to support military operations in urban terrain. The volume of data involved precludes wireless transmission and manual observation of all sensor feeds. Instead, local automatic processing of video feeds is required. By co-locating processors with video cameras, the bandwidth required to effectively support military operations can be reduced to manageable levels. Combat zones That See intends to track all vehicles that move within an extended area of observation. Despite the decreasing cost of cameras, processors, and communications, the complete observation of an entire metropolitan area is not practical. Hence, it will be necessary to develop vehicle-

association technology that permits reliable tracking of individual vehicles, using cameras whose Fields of View (FOV) do not overlap.

Source: DARPA. Proposer Information Pamphlet (PIP). "Combat Zones That See (CTS)." Broad Agency Announcement 03-15 (BAA 03-15) see Wayback Machine http://web.archive.org/web/20060619124609/http://dtsn.darpa.mil/ixo/solicitations/CTS/file/BAA_03-15_CTS_PIP.pdf and Noah Shachtman. "Big Brother Gets a Brain: The Pentagon's Plan for Tracking Everything That Moves." *Village Voice* July 9-15, 2003, http://www.villagevoice.com/news/0328,shachtman,45399,1.html

### Combined Intelligence Watch Center

Also known as the Combined Intelligence Center (CIC). Serves is the indications and warning center for worldwide threats from space, missile, and strategic air activity, as well as geopolitical unrest that could affect North America and U.S. forces/interests abroad. The center's personnel gather intelligence information to assist all the Cheyenne Mountain work centers in correlating and analyzing events to support NORAD and US Space Command decision makers.

Source: FAS. "Cheyenne Mountain Complex." http://www.fas.org/nuke/guide/usa/c3i/cmc.htm

### Command and Control Warfare

The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations. Also called C2W. C2W is both offensive and defensive: a. C2-attack.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

### Common Terrorism Information Sharing Standards

The CTISS program integrates information exchange standards, based on common ISE business processes and developed through the DOJ and DHS NIEM program management office, into new ISE-wide functional standards. NIEM epitomizes a successful Federal, State, local, tribal, and private sector initiative and provides a foundation for nationwide information exchanges leveraging data exchange standards efforts successfully implemented by the Global Justice Information Sharing Initiative. NIEM is also being strongly embraced by the private sector technology community.

Source: ISE, *Annual Report to Congress on the Information Sharing Environment* 2008, http://www.fas.org/irp/agency/ise/2008report.pdf

**Communicate**
To use any means or method to convey information of any kind from one person or place to another.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Communications Cover**
***See Information Superiority***

Concealing or altering of characteristic communications patterns to hide information that could be of value to an adversary.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Communications Intelligence Database**
The aggregate of technical information and intelligence derived from the interception and analysis of foreign communications (excluding press, propaganda, and public broadcast) used in the direction and redirection of communications intelligence intercept, analysis, and reporting activities.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Communications Security**
Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications.

Source: DoD. National Industrial Security Manual (NISPOM). DoD 5220.22-M, February 28, 2006, http://www.fas.org/sgp/library/nispom.htm

**Comparmentalization**
A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, Instruction 4009. June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Compartmentation**

Establishment and management of an organization so that information about the personnel, internal organization, or activities of one component is made available to any other component only to the extent required for the performance of assigned duties.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Compartmented Mode**

Mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following: (a) valid security clearance for the most restricted information processed in the system; (b) formal access approval and signed nondisclosure agreements for that information which a user is to have access; and (c) valid need-to-know for information which a user is to have access.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, Instruction 4009. *National Information Assurance Glossary* June, 2006., http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Compromise**

The disclosure of classified information to persons not authorized access thereto.

Source: U.S. Department of Justice. United States Marshals Service. Office of Inspections. Internal Security Division. *Information Security*. Washington D.C.: 1991. SUDOC: J 25.2: In 3

**Compromised**

***See Classified Matter***

A term applied to classified matter, knowledge of which has, in whole or in part, passed to an unauthorized person or persons, or which has been subject to risk of such passing.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Compromising Emanations**

Intentional or unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose national security information transmitted, received, handled, or otherwise processed by any information processing equipment. Compromising emanations consist of electrical or

acoustical energy emitted from within equipment or systems (e.g., personal computers, workstations, facsimile machines, printers, copiers, typewriters) which process national security information.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/fam/

**Computer Security Act Sensitive Information**

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 5 USC552a (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." Reference Public Law 100-235, The Computer Security Act of 1987, which is concerned with protecting the availability and integrity as well as the confidentiality of information.

Source: Centers for Disease Control. "Manual Guide - Information Security CD.C.-02."
Office of Security and Emergency Preparedness "Sensitive But Unclassified Information." 07/22/2005, http://www.fas.org/sgp/othergov/cD.C.-sbu.pdf.

**CONARC Incident Files**

**See *Counterintelligence Analysis Branch (CIAB) Compendium, Counterintelligence Field Activity, Counterintelligence Records Information System (CRIS)***

A collection of weekly or bi-weekly summaries known as the *CRIS Reports*. (p.46)

The CONARC File system duplicates the Intelligence Command System. (p.50)

Source: United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Army Surveillance of Civilians: A Documentary Analysis* by the staff of the Subcommittee on Constitutional Rights, Committee on the Judiciary, United States Senate. Washington, U.S. Government Printing Office, 1972, Y 4.J 89/2:AR 5/3, available at The Memory Hole, http://www.thememoryhole.org/2009/05/army-surveillance/

**Confidential**

***See Classification***

Criminal intelligence reports not designated as sensitive; and Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404

**Confidential Business Information | Business Proprietary Information**

1. The Toxic Substances Control Act (TSCA) allows chemical manufacturers and others who manufacture or market chemical-related substances and products to withhold information that is considered proprietary or a trade secret.
The term confidential business information means trade secrets or confidential commercial or financial information under FIFRA section 10(b) or 5 U.S.C. 552(b) (3) or (4). Also known as "Sensitive Business Information" and "Trade Secret Information."

Source: Environmental Protection Agency. "Special Review Procedures." 40 CFR 154.3, http://www.gpoaccess.gov/cfr/index.html

2. Documents that can be disclosed may be subject to confidentiality protection so as to completely thwart the purpose of disclosure.

Source: Jacqueline M. Warren. "Problems Encountered with Confidentiality Bars on Toxic Substances Disclosure Imposed by Federal Environmental Statutes." *New York University Environmental Law Journal* 2 no. 2 (1993): 292-299. http://www1.law.nyu.edu/journals/envtllaw/issues/vol2/index.html

3. When the FOIA was enacted, Congress recognized the need to protect confidential business information, emphasizing that a federal agency should honor the promises of confidentiality given to submitters of such data because "a citizen must be able to confide in his government."

Source: DOJ. FOIA Update. "Protecting Business Information." http://www.usdoj.gov/oip/foia_updates/Vol_IV_4/page1.htm

4. The U.S. International Trade Commission allows businesses submitting certain business data to mark the data as *confidential business information* or *business proprietary information*. Both terms have the same definition, but there are some differences in how the Commission applies the terms in practice. See generally Inspector General, U.S. International Trade Commission, Inspection Report No. 02-98, and Review of Commission Policies for Marking Controlled Data,

Confidential business information is information which concerns or relates to the trade secrets, processes, operations, style of works, or apparatus, or to the production, sales, shipments, purchases, transfers, identification of customers, inventories, or amount or source of any

income, profits, losses, or expenditures of any person, firm, partnership, corporation, or other organization, or other information of commercial value, the disclosure of which is likely to have the effect of either impairing the Commission's ability to obtain such information as is necessary to perform its statutory functions, or causing substantial harm to the competitive position of the person, firm, partnership, corporation, or other organization from which the information was obtained, unless the Commission is required by law to disclose such information. The term ``confidential business information'' includes ``proprietary information'' within the meaning of section 777(b) of the Tariff Act of 1930 (19 U.S.C. 1677f (b)). Nonnumerical characterizations of numerical confidential business information (e.g., discussion of trends) will be treated as confidential business information only at the request of the submitter for good cause shown.

Source: U.S. International Trade Commission. 19 CFR § 201.6(a). 19 CFR § 207.7(a) (1). See also 19 USC § 1332(g), 19 USC § 1673e(c) (4) (A), http://www.gpoaccess.gov/CFR/index.html and http://www.usitc.gov/oig/OIG-IR-02-98.pdf

### Confidential-Cleared U.S. Citizen

A citizen of the United States who has undergone a background investigation by an authorized U.S. Government Agency and been issued a Confidential security clearance in accordance with Executive Orders 12968 and 10450 and implementing guidelines and standards published in 32 CFR Part 147.

Source: U.S. Department of State. Foreign Affairs Manual. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/fam/

### Confidential Commercial Information

Records provided by a submitter that may contain material exempt from release under the FOIA because disclosure could reasonably be expected to cause the submitter substantial competitive harm.

Source: "Public Availability of Records." 36 CFR 1250.2, http://www.gpoaccess.gov/CFR/index.html

### Confidentiality

Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Source: Committee for National Security Systems (CNSS). Instruction 4009. National Information Assurance Glossary, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

### Confidential Source

Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

**Confirmation of Information (Intelligence)**
An information item is said to be confirmed when it is reported for the second time, preferably by another independent source whose reliability is considered when confirming information.

Source: DoD. *DoD Dictionary of Military and Associated Terms*. Joint Publication 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**Confusion Agent**
An individual who is dispatched by the sponsor for the primary purpose of confounding the intelligence or counterintelligence apparatus of another country rather than for the purpose of collecting and transmitting information.

Source: *DoD Dictionary of Military and Associated Terms*. Joint Publication 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**[National Intelligence Program] Congressional Budget Justification Books (CBJBs)**
*See Operational Files*

1. Justification materials on national programs are submitted to the two intelligence committees along with classified CBJBs, which include one volume for each NIP program plus an additional summary volume. The classified books, available to Members and committee staff, include explanatory narrative and resource displays for all resources requested by the program. Also included are descriptions of base levels of efforts, ongoing initiatives and new initiatives with associated resource displays. CBJBs are submitted to Congress within a few weeks of the delivery of the budget in early February and form the basis for the committees' review of the entire NIP prior to the drafting of annual intelligence authorization bills.

Classified budget justification books, provided by the Administration to Congress, are the primary ways, in addition to oral testimony, by which Congress obtains information about intelligence programs. In 1997 HPSCI [House Permanent Select Committee on Intelligence] criticized justification books for lacking "several critical components necessary for the Committee to ensure proper alignment of funding within the funding appropriations categories.

Clear identification of each project; its specific budget request numbers; the appropriation category (e.g., Other Procurement, Defense-wide; RDT&E, Navy, etc.); the budget request line number, and if a research and development project, the Program Element number [are] essential to this task....

Source: Richard A. Best, Jr. "Intelligence, Surveillance, and Reconnaissance (ISR) Programs: Issues for Congress." *CRS Report to Congress February* 22, 2005. http://www.fas.org/sgp/crs/intel/RL32508.pdf and DoD Financial Management Regulation Volume 2B, Chapter 16 "Intelligence Programs/Activities." June 2004, http://www.dod.mil/comptroller/fmr/02b/02b_16.pdf.

2. The Committee [Permanent Select Committee on Intelligence] has become increasingly frustrated with the lack of detail provided in the project descriptions in the National Foreign Intelligence Program (NFIP) CBJBs. Further, the Committee believes that the financial management practices at some NFIP agencies are so inadequate that specific project-level financial information is not even well known corporately. For example, in preparation for the budget authorization, the Committee had to, once again ask representatives from CIA and NSA to provide additional programmatic information on their systems development activities--basic information that apparently was not readily available.

If NFIP agencies are unable to provide detailed financial data for the congressional oversight process, the Committee questions whether they have the detail necessary to make sound investment decisions.

The Committee, therefore, expects a change to the format and content of the NFIP budget submission. Specifically, the Committee wants all future NFIP CBJBs to provide the following information on each project valued at $1.0 million or more (including systems developed by government personnel):

project mission description and budget item justification;
key performance characteristics and requirements;
organizations providing management oversight;
customers and products associated with the project;
contract information;
budget breakout by program element number (RDT&E, Procurement, O&M) for the two proceeding fiscal years, the budget year, the FYDP, and cost to complete;
civilian and military manpower numbers and costs;
program highlights/planned program by type of funding (RDT&E, Procurement, O&M) for the two preceding years, the budget year, and one year beyond the budget year;
project budgetary change summary and explanation;
related program funding summary; and,

the project milestone schedule.

Source: Intelligence Authorization Act for Fiscal Year 2001, http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr620&dbname=106&

3. Freedom of Information Act proceeding in which plaintiff pro se Steven Aftergood seeks disclosure of unclassified portions of the National Reconnaissance Office (NRO) Congressional Budget Justification Book for Fiscal Year 2006. The requested information has been withheld by defendant NRO on grounds that the requested record is an "operational file" that is exempt from FOIA processing under 50 U.S.C. § 403-5e.

Source: *Steven Aftergood v. National Reconnaissance Office*. Case No. 05-1307 (RBW), http://www.fas.org/sgp/foia/nro-cbjb/sa120505.pdf and Judge Walton's ruling in *Steven Aftergood v. National Reconnaissance Office,* D.C. District Case No. 05-1307, http://www.fas.org/sgp/foia/nro-cbjb/rbw072406.pdf

## Conspiracy Theories

Belief that powerful, evil hidden forces are secretly manipulating the course of world events and history.

Conspiracy theories are similar to urban legends, but center around the idea that powerful, evil hidden forces are secretly manipulating the course of world events and history and that nothing is as it seems… inconvenient facts such as these are regularly ignored or dismissed by conspiracy theories in favor of extraordinarily complex and convoluted conspiracies, for which there is no evidence, merely uninformed speculation. Nevertheless, by blaming powerful alleged villains, conspiracy theories find a wide audience for whom suspicions are much more powerful in forming beliefs than logic, reason, or facts.

Source: U.S. State Department. International Information Programs. "Definitions." http://www.america.gov/st/pubs-english/2005/January/20050114144833atlahtnevel0.1894342.html and National Security Council. "Subcultures of Conspiracy and Misinformation." National Strategy for Combating Terrorism, http://www.globalsecurity.org/security/library/policy/national/nsct_sep2006_sectionv.htm

## Content Management

The process of capturing and creating, managing and storing, and delivering the substantive details of structured and unstructured data.

Source: Director of Central Intelligence Directive 8/1. "Intelligence Community Policy on Intelligence Sharing." June 4, 2004, http://www.fas.org/irp/offdocs/D.C.id8-1.html

## Contractor Access Restricted Information

Unclassified information that involves functions reserved to the federal government as vested by the Constitution as inherent power or as implied power as necessary for the proper performance of its duties. In many instances, CARI prevents contractors from making decisions that would affect current or future contracts and procurement procedures, primarily during pre-award activities.

Source: Centers for Disease Control. "Manual Guide - Information Security CD.C.-02." Office of Security and Emergency Preparedness "Sensitive But Unclassified Information." 07/22/2005, http://www.fas.org/sgp/othergov/cD.C.-sbu.pdf.

## Control

1. Authority of the agency that originates information, or its successor in function, to regulate access to the information.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

2. The Department's legal authority over a record, taking into account the ability of the Department to use and dispose of the record as it sees fit, to legally determine the disposition of a record, the intent of the record's creator to retain or relinquish control over the record, the extent to which Department personnel have read or relied upon the record, and the degree to which the record has been integrated into the Department's record keeping system or files.

Source: 22 CFR 171. "Foreign Relations, Department of State." http://www.gpoaccess.gov/CFR/index.html (a detailed list of records that are exempt under 5 U.S.C. 552a (k) (1). "The reason for invoking this exemption is to protect material required to be kept secret in the interest of national defense and foreign policy").

## Controlled Access Area

Specifically designated areas within a building where classified information may be handled, stored, discussed, or processed.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/fam/

## Controlled Dossier

Files of a particularly sensitive nature due to substantive content or method of collection, which are physically segregated from the body of ordinary materials.

Source: DoD. Army Regulation AR381-45. "Investigative Records Repository," August 25, 1989., http://www.army.mil/usapa/epubs/pdf/r381_45.pdf

**Controlled Information**

1. Information conveyed to an adversary in a deception operation to evoke desired appreciations.

2. Information and indicators deliberately conveyed or denied to foreign targets to evoke invalid official estimates that result in foreign official actions advantageous to US interests and objectives.

Source: DoD. *The Department of Defense Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Controlled Unclassified Information**

***See Sensitive But Unclassified, Unclassified Information***

**Note:** See Gen. Clapper's policy directive April 7, 2009, "Clarification of Current DoD Policy on Controlled Unclassified Information (CUI)." http://www.fas.org/sgp/cui/ousd040709.pdf

1. Unclassified information to which access or distribution limitations have been applied according to national laws, policies and regulations of the U.S. government. These types of information include, but are not limited to: patent secrecy data, confidential medical records, inter- and intra-agency memoranda which are deliberative in nature, data compiled for law enforcement purposes, data obtained from a company on a confidential basis, employee personal data, Privacy Act information, internal rules and practices of a government agency, which if released, would circumvent an agency policy and impede the agency in the conduct of its mission.

Source: Department of the Army. Army Regulation 380-10, "Foreign Disclosure and Contacts with Foreign Representatives," June 22, 2005, http://www.fas.org/irp/DoDdir/army/ar380-10.pdf, FAS, "U.S. Army's Concerns with Protection of Controlled Unclassified Information," August 15, 2008, http://www.fas.org/sgp/othergov/dod/dib-cui.pdf, Daniel Wasserbly, "Army Cyber Task Force To Manage Growing Industrial Espionage Risk," *Inside the Army*, October 20, 2008, http://defensenewsstand.com/insider.asp?issue=10202008sp, FAS *International Programs Security Handbook* Chapter 4. Office of the Deputy to the Under Secretary of Defense (Policy) for Policy Support, 1993, http://www.fas.org/sgp/library/ipshbook/Chap_04.html and http://www.fas.org/sgp/library/ipshbook/app_g.html

2. Controlled Unclassified information (CUI) is the categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is:

- pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government
- under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination

Source: National Archives and Records Administration, Controlled Unclassified Information Office, http://www.archives.gov/cui/

3. `(1) CONTROLLED UNCLASSIFIED INFORMATION- The term `controlled unclassified information' means a categorical designation that refers to unclassified information, including unclassified information within the scope of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), including unclassified homeland security information, terrorism information, and weapons of mass destruction information (as defined in such section) and unclassified national intelligence (as defined in section 3(5) of the National Security Act of 1947 (50 U.S.C. 401a(5))), that does not meet the standards of National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or National Archives and Records Administration policy requires safeguarding from unauthorized disclosure, special handling safeguards, or prescribed limits on exchanges or dissemination.

Source: H.R. 6193, ""Improving Public Access to Documents Act of 2008," http://thomas.loc.gov/cgi-bin/query/F?c110:16:./temp/~mdbsVhieaJ:e19883:; I can't tell if this was passed by the Senate http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.06193: ; also see Open the Government.org, http://www.openthegovernment.org/article/articleview/49/1/16 and DoD, eliminating SBU for CUI, http://www.ombwatch.org/article/articleview/4140/

3. Creates a single policy for the government, reducing over 100 different SBU markings to three:

Standard Safeguarding and standard Dissemination;

Standard Safeguarding and specified Dissemination; and

Enhanced Safeguarding and Specified Dissemination.

Describes the mandatory standards for the designating, marking, safeguarding, and disseminating of all controlled unclassified terrorism-related information originated by the Federal Government and shared within the ISE, regardless of the medium used for its display,

storage, or transmittal;31 and  Strongly encourages its adoption by SLT and private sector entities.

On May 9, 2008, the President issued a memorandum requiring agencies to implement the CUI framework. In addition, the President designated the National Archives and Records Administration (NARA) as the Executive Agent. NARA, in coordination with a CUI Council, will govern the new Framework and oversee its implementation.

Source: Program Manager, Information Sharing Environment. *Annual Report to Congress on the Information Sharing Environment*, June 30 2008, http://www.ise.gov/docs/reports/Annual-Report-to-Congress-20080702.pdf

### Controlled Unclassified Information Office

The mission of the Controlled Unclassified Information Office (CUIO) is to oversee and manage the implementation of the CUI Framework to accomplish the dual objectives of improving the sharing of vital information with our Nation's defenders who need it while also protecting the privacy and other legal rights of Americans…

- Develop and issue CUI policy standards and implementation guidance consistent with the Presidents Memorandum, including appropriate recommendations to State, local, tribal, private sector, and foreign partner entities for implementing the CUI Framework.
- Establish new safeguarding and dissemination controls, as appropriate, and upon a determination that extraordinary circumstances warrant the use of additional CUI markings, authorize the use of such additional markings.
- Establish and chair the CUI Council.
- Establish, approve, and maintain safeguarding standards and dissemination instructions including, "Specified Dissemination" requirements proposed by the head of departments and agencies.

Source: National Archives and Records Administration, Controlled Unclassified Information Office, http://www.archives.gov/cui/

### Copyright

***See Patents, Trademarks, Trade Secrets***

Copyright is but one of five principal forms of American intellectual property ("IP") law, a category that includes trademarks, patents, trade secrets, and licenses.

Source: K. Matthews Dames, "The copyright landscape" *Online* September 1, 2006, http://www.allbusiness.com/legal/intellectual-property-law-copyright/10548080-1.html

**Copyright Law of the United States of America**
A form of protection provided to the authors of "original works of authorship" including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished. The 1976 Copyright Act generally gives the owner of copyright the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phonorecords of the copyrighted work, to perform the copyrighted work publicly, or to display the copyrighted work publicly.

The copyright protects the form of expression rather than the subject matter of the writing. For example, a description of a machine could be copyrighted, but this would only prevent others from copying the description; it would not prevent others from writing a description of their own or from making and using the machine. Copyrights are registered by the Copyright Office of the Library of Congress.

Source: United States Copyright Office. "General Information Concerning Patents." http://www.uspto.gov/web/offices/pac/doc/general/#copyright

**Counterinformation**
Actions dedicated to controlling the information realm.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995. [At the Wayback Machine, http://web.archive.org/web/20040901091302/http://www.af.mil/lib/corner.html]

**Counter-Information Team**
***See Bureau of International Information Programs, Public Diplomacy***
"In coordination with the CIA, FBI and others, the team helps U.S. embassies identify and rebut other nations' disinformation, most often fabrications about the United States planted in foreign newspapers or television shows and, these days, on the Internet."

Source: Sourcewatch, http://www.sourcewatch.org/index.php?title=Counter-Information_Team

**Counterintelligence**
1. Information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Source: National Security Act of 1947, as amended (50 U.S.C. Chapter 15, 401(a) ,http://www.gpoaccess.gov/uscode/browse.html and Executive Order 12333, 3.4. "United States

Intelligence Activities."
http://www.archives.gov/federal-register/executive-orders/1981-reagan.html

2. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Marine Corps) Within the Marine Corps, counterintelligence constitutes active and passive measures intended to deny threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545-b.htm

3. As defined in Executive Order 12333, includes "information gathered" and "activities conducted" in order to "to protect against espionage, other intelligence activities, sabotage or assassination conducted on behalf of foreign powers, organizations, or persons, or international terrorist activities but not including personnel, physical documents or communications security."

Source: Executive Order 12333, http://www.archives.gov/federal-register/executive-orders/1981-reagan.html, and U.S. Department of Defense. "DoD Counterintelligence Functional Services," DoD Instruction 5240.16, May 21, 2005, http://www.fas.org/irp/DoDdir/DoD/i5240_16.pdf

**Counterintelligence Analysis Branch (CIAB) Compendium**

***See Counterintelligence Field Activity, Law Enforcement Intelligence Units***

Both volumes which were classified "SECRET," are entitled *Civil Disturbances and Dissidence*, Volume 1 is subtitled *Cities and Organizations of Interest* . Volume 2 subtitled *Personalities of Interest*. Both were prepared by the Counterintelligence Analysis Branch (CIAB) and bear the imprint of Headquarters, Department of the Army; Office of the Assistant Chief of Staff for Intelligence." Each opens with an acknowledgement that the basic information on organizations and individuals contained therein was provided primarily by the Federal Bureau of Investigation.

The Compendium employed a loose-leaf format to facilitate the continual updating of information. Standardized formats were prescribed to assure uniformity in the presentation of significant data. New information was to be interested in the form of replacement pages. Users were encouraged to forward any information in their possession which could fill existing gaps or add substantive knowledge to the present treatment of any city, organization, or personality covered. (p.10)

In speaking of surveillance of the American Friends Services Committee and "black organizations," the report states (p.12): "Allegations of possible subversive influence appear frequently [sic, in the Compendium], usually without reference to the source of the charge , the evidence on which it is based, or any explanation of what constitutes a 'subversive group' or 'communist front.'" Several paragraphs later, the report continues "…the Army indiscriminately lumped together organizations of unquestioned legitimacy and legality (even in the eyes of the Army) together with those few groups popularly regarded as having employed unlawful methods in pursuit of their ends. In no case, however, was there proof that even these latter groups had violated the law, let alone that they constituted any threat to national security."

Numerous copes of the *Compendium* were allegedly destroyed after a 1970 *Chicago Sun Times* (p.20) article broke news regarding the document, "but this has not been assured."

Source: Source: Alan LeMond and Ron Fry. *No Place to Hide*. New York: St. Martin's Press, 1975, United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Army Surveillance of Civilians: A Documentary Analysis* by the staff of the Subcommittee on Constitutional Rights, Committee on the Judiciary, United States Senate. Washington, U.S. Government Printing Office, 1972, Y 4.J 89/2:AR 5/3, available at The Memory Hole, http://www.thememoryhole.org/2009/05/army-surveillance/

**Counterintelligence Analytical Research Data System (CARDS)**
***See Data Mining***
Department of Energy's Inventory of Data Mining Efforts. Is used to log briefings and debriefings given to DOE employees who travel to foreign countries or interact with foreign visitors to DOE facilities. Data are mined to identify potential threats to DOE assets;
Purpose: Detecting criminal activities or patterns;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. Data Mining: Federal Efforts Cover a Wide Range of Uses. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Counterintelligence Automated Investigative Management System (CI-AIMS)**
***See Data Mining***
Department of Energy's Inventory of Data Mining Efforts. Is an investigative management system used by Department of Energy (DOE) field sites to track investigative cases on

individuals or countries that threaten DOE assets. Information stored in this database is also used to support federal and state law enforcement agencies in support of national security;
Purpose: Detecting criminal activities or patterns;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: No.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

### Counterintelligence Collection

The systematic acquisition of information concerning espionage, sabotage, terrorism, other intelligence activities or assassinations conducted by or on behalf of terrorists, foreign powers, and other entities.

Source: DoD. "DoD Counterintelligence Collection Reporting." DoD 5240.17. October 26, 2005,http://www.fas.org/irp/doddir/dod/i5240_17.pdf

### Counterintelligence Field Activity (CIFA)

***See Special Access Programs, Defense Counterintelligence and Human Intelligence Center***

1. The Defense Counterintelligence Field Activity (CIFA) is a transformation initiative created to lead the development of a "to-the-edge" counterintelligence system for the Department of Defense. Its mission is to produce a common Defense Department counterintelligence operational picture, and deliver unique and actionable information to key decision makers in federal, state and local governments.

4.2. The Department will make full use of advanced technology to create and maintain a collaborative CI analytic environment to protect critical DoD and national assets.

4.4 All DoD CI matters and activities that affect or are related to DoD Special Access Programs (SAPs) shall comply with the security procedures of Executive Order 12958 (reference (c)), DoD Directive O-5205.7 (reference (d)), and the DoD Overprint to the *National Industrial Security Program Operating Manual* Supplement (reference (e)).

6.2.8. Develop and integrate the Defense CI Information System (DCIIS) Program, including, but not limited to, the architecture, software development, training, implementation, and sustainment of the D.C.IIS while ensuring the architectural integrity of the system.

Source: NOTE: dead links – use the Wayback Machine @ http://www.archive.org/web/web.php – Defense Security Service (DSS), "Counterintelligence to the Edge," http://www.dss.mil/polygraph/cifa.htm and DoD Directive 5105.67, "Department of Defense Counterintelligence Field Activity (DoD CIFA)," 02/19/2002, http://www.dtic.mil/whs/directives/corres/html2/d510567x.htm; Also see Jeffrey Richelson's *The Pentagon's Counterspies: The Counterintelligence Field Activity (CIFA)* Electronic Briefing Book @ the National Security Archive, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/index.htm

2. On August 3, 2008, all DoD CIFA CI missions, responsibilities, functions, and authorities as well as all associated resources including all personnel, support contracts and contractors, and appropriate records and archives shall transition in place to DIA. Personnel transfer notifications, as appropriate and required, shall be accomplished in advance of the August 3, 2008 transfer from DoD CIFA to DIA

Source: DoD. Deputy Secretary for Defense, "Establishment of the Defense Counterintelligence and Human Intelligence Center (D.C.HC)," DTM 08-032, July 22, 2008, http://www.fas.org/irp/doddir/dod/D.C.hc.pdf

**Counterintelligence Records Information System (CRIS)**

***See CONARC Incident Files, Counterintelligence Analysis Branch (CIAB) Compendium, Counterintelligence Field Activity, Law Enforcement Intelligence Units***

1. Also called the Fort Monroe Data Bank. "It contained thee basic categories of information with a cross-reference capability among them. The categories were incidents, personalities, and organizations…information for all three files was received from the five continental armies and the Military District of Washington (CONUSAMDW), the Intelligence Command, and the FBI. Each of these three collection systems, in turn, gathered information from state and municipal police departments and the news media" (p.45).

Volumes 2-6 "Personalities edition" contain 2,269 pages of detailed summaries of the political beliefs and activities of nearly 5,000 people, in addition to a 99-page index to persons listed (p.51).

p. 72 of the report details the Fort Hood "computerized storage system for civil disturbance and intelligence."

Source: United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Army Surveillance of Civilians: A Documentary Analysis* by the staff of the Subcommittee on Constitutional Rights, Committee on the Judiciary, United States Senate. Washington, U.S. Government Printing Office, 1972, Y 4.J 89/2:AR 5/3, available at The Memory Hole, http://www.thememoryhole.org/2009/05/army-surveillance/

2. CRIS was established in January 1968, and computerized in May.

Source: Alan LeMond and Ron Fry.*No Place to Hide*. New York: St. Martin's Press, 1975. 229.

**Counterterrorism Communications Center**

An interagency initiative to develop and deliver effective messages to undermine ideological support for terror and to counter terrorist propaganda. The Center [sic, U.S. department of State] provides leadership and coordination for interagency efforts in the war of ideas and seeks to integrate and enhance the U.S. Government's diverse public diplomacy counterterrorism efforts.

Source: U.S. Senate Committee on Homeland Security and Governmental Affairs, "Violent Islamist Extremism: Government Efforts to Defeat It," Statement of Jeremy Curtin, Coordinator, Bureau of International Information Programs, U.S. Department of State, May 10, 2007, http://www.investigativeproject.org/documents/testimony/284.pdf

**Country Tap**

In speaking of NSA's warrantless (emails and phone) surveillance of U.S. citizens as a counterterrorism measure, Dr. Brian Reid with the Electronic Frontier Foundation observed: "This is not a wiretap, this is a *country-tap*" [emphasis added].

Source: Keith Perine, "Judiciary Postpones Decision on Telecom Immunity in Considering FISA Bill." http://www.eff.org/pages/news-coverage-mark-klein-washington and EFF, "NSA Spying," http://www.eff.org/issues/nsa-spying

**Court-Legal-Litigation Records Related**

***See Pacer, Record, Records***

1. Generally considered public records, are published and are available from the courts. The Supreme Court has found a qualified First Amendment right of access to criminal trials and to records directly related to criminal trials. Types of court records (most definitions taken from Nolo.com):

- Brief: A document used to submit a legal contention or argument to a court.
- Discovery documents: Used in pretrial information gathering, most federal and state courts are not requiring litigants to file copies of pretrial depositions, interrogatories and other documents (Federal Rules of Civil Procedure 5 (d) ); it has been argued that the pretrial disclosure process is not a public matter (*Seattle Times v. Rhinehart*, 1984)
- Grand Jury records: There is no First Amendment right of access to grand jury proceedings. Grand juries operate traditionally and statutorily under strict secrecy rules.

The Supreme Court has repeatedly cited several reasons for grand jury secrecy, including the need to protect the innocent accused who is exonerated. This is, at least in part, a privacy interest, and one of a few privacy interests that can be clearly identified as a foil to the First Amendment access interests in the criminal justice system.

Source: Taken in part from Robert Gellman, "Public Records: Access, Privacy, and Public Policy: A Discussion Paper." http://www.cdt.org/privacy/pubrecs/pubrec.html, David S. Sanson. "The Pervasive Problem of Court-Sanctioned Secrecy and the Exigency of National Reform." 53 Duke L. J. 807 http://www.law.duke.edu/journals/dlj/articles/dlj53p807.htm, Center for Democracy and Technology. "A Quiet Revolution in the Courts: Electronic Access to State Court Records," http://www.cdt.org/publications/020821courtrecords.shtml, and Rocky Mountain Chapter, Sierra Club. "Rocky Flats Grand Jury Report Published," http://rmc.sierraclub.org/rocky.shtml

*Juror records*: In some states, personal juror records are sealed by the court at the conclusion of a criminal trial.

*Juvenile records*: In most states, juvenile court proceedings (individuals less than 21 years old) are closed to the press and public.

*Memdispos* (Memorandum Dispositions or Unpublished Opinions): Pursuant to Ninth Circuit Rule 36-3, not published in the *Federal Reporter*, nor do they have precedential value. Memdispos cannot be cited and are very controversial within the legal field.

Source: Deborah Jones Merritt and James J. Brudney "Stalking the Secret Law: What Predicts Publications in the United States Courts of Appeals." *Vanderbilt Law Review* 54 (2001): 71, Alex Kozinski and Stephen Reinhardt. "Please Don't Cite This: Why We Don't Allow Citation to Unpublished Opinions." http://www.nonpublication.com/don't%20cite%20this.htm, "*Sorchini v. City of Covina*: Concerning Unpublished Judicial Opinions," http://www.fas.org/sgp/news/2001/05/sorchini.html

Official reports: court reports directed by statute

- Sealed: Records determined by either the Court or parties, to be too sensitive to be made public.
- Unofficial reports: published without statutory direction

2. A bill to amend chapter 111 of title 28, United States Code, relating to protective orders, sealing of cases, disclosures of discovery information in civil actions, and for other purposes. The purpose of S. 2449, the Sunshine in Litigation Act, is to protect the public from potential health or safety dangers that are too often concealed by court orders restricting disclosure of information.

Source: United States. Congress. Senate. Committee on the Judiciary. Sunshine in Litigation Act of 2008: report (to accompany S. 2449). Washington, D.C.: U.S. G.P.O., 2008, http://purl.access.gpo.gov/GPO/LPS99664

### Covert Products

A-5. Covert products require exceptional coordination, integration, and oversight. The operations are planned and conducted in such a manner that the responsible agency or government is not evident, and if uncovered, the sponsor can plausibly disclaim any involvement. Gray and black products are employed in covert operations.
Source: DoD *Psychological Operations,* FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

### Criminal Intelligence

Data which has been evaluated to determine that it is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity. [Certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area].

Source: Judicial Administration. 28 CFR 23, http://www.gpoaccess.gov/CFR/index.html

### Criminal Intelligence System

Arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

Source: Department of Justice. "Criminal Intelligence Information Operating Systems." 28 CFR 23.3(b)(1) , http://www.gpoaccess.gov/CFR/index.html

### Criminal Investigation Division Data Mining

U.S. Secret Service. Mines data in suspicious activity reports received from banks to find commonalities in data to assist in strategically allocating resources;
Purpose: Detecting criminal activities or patterns;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Critical and Sensitive Information List**

A list containing the most important aspects of a program or technology, whether classified or unclassified, requiring protection from adversary exploitation.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

**Critical Energy Infrastructure Information (CEII)**

CEII is information concerning proposed or existing critical infrastructure (physical or virtual) that:

> Relates to the production, generation, transmission or distribution of energy;
> Could be useful to a person planning an attack on critical infrastructure;
> Gives strategic information beyond the location of the critical infrastructure.

CEII Is exempt from mandatory disclosure under the Freedom of Information Act.

Source: Federal Energy Regulatory Commission (FERC). http://www.ferc.gov/legal/ceii-foia/ceii.asp and FERC/DOE. "Information Requests." 18 CFR 388.113, http://www.gpoaccess.gov/CFR/index.html

**Critical Information**

1. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries or competitors for them to plan and act effectively to guarantee failure or unacceptable consequences for mission accomplishment.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995. http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf and Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Critical Infrastructure Information (CII)**

***See Freedom of Information Act Exemptions, National Asset Database***

1. Critical Infrastructure has the definition referenced in section 2 of the Homeland Security Act of 2002 and means systems and assets, whether physical or virtual, so vital to the

United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems-

> (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;
>
> (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or
>
> (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Source: Department of Homeland Security PCII
http://www.dhs.gov/dhspublic/display?theme=52&content=3455 ;
Critical Infrastructure Information Act of 2002 (Title II Subtitle B, Homeland Security Act of 2002, 6 U.S.C. 131-134), http://www.dhs.gov/interweb/assetlibrary/CII_Act.pdf
and Coalition of Journalists for Open Government,
http://www.cjog.net/protest_critical_infrastructure_i.html and Department of Homeland Security. "Protected Critical Infrastructure Information." 6 CFR 29.2, http://www.gpoaccess.gov/cfr/index.html

2. A New Jersey resident, requesting access to a township's electronic map of land parcels, has brought to light the first public example of a law that hides information that meets standards for "critical infrastructure information" (CII). The local municipal utility denied the resident's request for land parcel information, because the data had been protected by the Department of Homeland Security (DHS) under the CII program.

Source: OMB Watch. "First Public Case of Critical Infrastructure Information." August 8, 2005,
http://www.ombwatch.org/article/articleview/2977/1/355

## Critical Intelligence

Information of such urgent importance to the security of the United States that it is directly transmitted at the highest priority to the President and other national decisionmaking officials before passing through regular evaluative channels. In the military it is intelligence that requires the immediate attention of the commander. It includes, but is not limited to: (a) strong indications of the immediate outbreak of hostilities of any type (warning of attack); (b) aggression of any nature against a friendly country; (c) indications or use of nuclear/biological chemical weapons (targets); and (d) significant events within potential enemy countries that may lead to modifications of nuclear strike plans.

Source: Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C.: Springfield, VA: National Technical Information Service, [1999?]. SUDOC: PREX 3.2:C 76 and PREX 3.2/2:G 94

## Critical Oversight Information

***See Sensitive Security Information***

Information that speaks to the quality and integrity of their performance as policy makers, managers or employees of our seaports, airports and transit systems. It is budget information and details on revenue and spending. It is information about personnel and their qualifications, training and performance. It is information about the construction and maintenance of new public assets, including the myriad change orders that seem an inevitable feature of the government contract process. It is information about deals with carriers and suppliers and vendors and tenants. It is also information about public convenience and use of the public areas -- and about personal safety…critical oversight information has a connection with security.

Source: Coalition of Journalists for Open Government, http://www.rcfp.org/news/documents/20040716-ssicomment.pdf

## Critical Program Information (CPI)

13.1 Critical Program Information or CPI, is defined as that "key" information about the program, technologies, and/or systems that if compromised would degrade combat effectiveness or shorten the expected life of the system. CPI may also provide insight into program vulnerabilities, countermeasures, and limitations. Unauthorized access to this information or systems could allow someone to kill, counter, and clone, negate, or degrade the system before or near the scheduled deployment, forcing a major design change to maintain the same level of effectiveness and capability. CPI may be classified or unclassified information. Given the potentially grave consequences that can result from the compromise of CPI, everyone who uses this sensitive information must ensure it is adequately identified and protected.

Source: Air Force Classification Guide for the Global Broadcast System, April 29, 2007, http://www.fas.org/sgp/othergov/dod/gbs.pdf

### CRS Publication Policy

The reasons for limiting public dissemination of our work can be summarized as follows. First, there is a danger that placing CRS, a legislative support agency, in an intermediate position, responding directly to constituents as members of the public, would threaten the dialog on policy issues between Members and their constituents that was envisioned by the Constitution as the essence of the representational role of Members. Leaving dissemination of CRS products to the discretion of Members avoids placing a "faceless bureaucracy" between constituents and their elected representative. (p.6)

Source: Access to CRS Reports *Memorandum* April 18, 2007, http://ftp.fas.org/sgp/crs/crs041807.pdf.

### Cryptographic Information

All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment (or their functions and capabilities) and all cryptomaterial.

Source: Department of Defense. *DoD of Military and Associated Terms*. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

### Cryptography

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

### Cultivation

A deliberate and calculated association with a person for the purpose or recruitment, obtaining information, or gaining control for these or other purposes.

Source: DoD. *The Department of Defense Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

### Cultural Diplomacy

Cultural diplomacy, which has been defined as "the exchange of ideas, information, art, and other aspects of culture among nations and their peoples in order to foster mutual understanding,"2 is the linchpin of public diplomacy; for it is in cultural activities that a nation's idea of itself is best represented...

Source: Milton C. Cummings, Jr. *Cultural Diplomacy and the United States Government: A Survey.* Washington, D.C.: Center for Arts and Culture, 2003 and Cultural *Diplomacy*
*The Linchpin of Public Diplomacy: Report of the Advisory Committee on Cultural Diplomacy.* U.S. Department of State, 2005, http://iwp.uiowa.edu/about/CulturalDiplomacyReport.pdf

**Custodian**
An individual who has possession of or is otherwise charged with the responsibility for safeguarding and accounting for classified information.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/fam/

**Cyberwar**
**See *Defensive Information Warfare, Direct Information Warfare, Information Warfare, Netwar, Strategic Information Warfare***

Refers to conducting military operations according to information-related principles. It means disrupting or destroying information and communications systems. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended.

This form of warfare may involve diverse technologies, notably for command and control, for intelligence collection, processing and distribution, for tactical communications, positioning, identifying friend-or-foe, and for "smart" weapons systems, to give but a few examples. It may also involve electronically blinding, jamming, deceiving, overloading and intruding into an adversary's information and communications circuits.

Source: John J. Arquilla and David F. Ronfeldt . "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict. " *Rand Research Review* xix no. 2 (1995),
http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html

## ~ D ~

### Daily Digest

A 10 to 15 page report which provides a global perspective on a single issue and is sent by 1:00 p.m. Monday through Friday to more than 750 senior and mid-level foreign policy officials. The format is the same as the *Early Report*. It is also transmitted electronically via e-mail and the Internet where it reaches an expanding audience in the foreign policy community of the U.S. Government, including the White House, the Departments of State, defense, Justice, treasury, and Commerce, the CIA and both Houses of Congress.

Source: Department of State. *Foreign Affairs Manual*. 10 FAM 413.2, "Office of Research." http://www.state.gov/m/a/dir/regs/

### Damage Assessment

A determination of the effect of a compromise of classified information on national security.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545-b.htm

### Damage Caused by Unauthorized Disclosure

The decision to apply classification involves two sub-elements, both of which require the application of "reasoned judgment on the part of the classifier":

A determination that the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security of the United States, and that the damage can be identified or described. it is not necessary for the original classifier to produce a written description of the damage at the time of the classification, but the classifier must be prepared to do so if the information becomes the subject of a classification challenge, a request for mandatory review for declassification, or a request under the Freedom of Information Act.

A determination of the probable operations, technological and resource impact of classification.

Source: National Imagery and Mapping Agency. *NIMA Guide to Marking Classified Documents*, October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

### Damage to the National Security

***See National Security***

Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

**Dark Web | Dark Web Terrorism Research**

1. The AI Lab Dark Web project is a long-term scientific research program that aims to study and understand the international terrorism (Jihadist) phenomena via a computational, data-centric approach. We aim to collect "ALL" web content generated by international terrorist groups, including web sites, forums, chat rooms, blogs, social networking sites, videos, virtual world, etc.

Source: AI Lab, University of Arizona, http://ai.arizona.edu/research/terror/index.htm

2. The University of Arizona's ultra-ambitious "Dark Web" project "aims to systematically collect and analyze all terrorist-generated content on the Web," the National Science Foundation notes. And that analysis, according to the Arizona Star, includes a program which "identif[ies] and track[s] individual authors by their writing styles

Source: Noah Shachtman,"Do You Write Like a Terrorist? *Wired* September 24, 2007, http://blog.wired.com/defense/2007/09/do-you-write-li.html

**Data**

The lowest class of information on the cognitive hierarchy. Data consist of raw signals communicated by any nodes in an information system, or sensings from the environment detected by a collector of any kind (human, mechanical, or electronic).

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545-b.htm

**Data Aggregation**

Compilation of unclassified individual data systems and data elements that could result in the totality of the information being classified or of beneficial use to an adversary.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Data Base**

Data base means a set of data, consisting of at least one data file, that is sufficient for a given purpose.

Source: National Archives and Records Administration. 36 CFR 1234.2, http://www.gpoaccess.gov/cfr/index.html

**Data Mining**

1. The science of extracting useful information from large data sets or databases.

Source: Jeffrey W. Seifert. "Data Mining: An Overview." *CRS Report for Congress* December 16, 2004. http://www.fas.org/irp/crs/RL31798.pdf & update, January 27, 2006, http://www.fas.org/sgp/crs/secrecy/RS20748.pdf

2. Application of database technology and techniques (such as statistical analysis and modeling) to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results.

Federal agencies are using data mining for a variety of purposes, ranging from improving service or performance to analyzing and detecting terrorist patterns and activities. Our survey of 128 federal departments and agencies on their use of data mining shows that 52 agencies are using or are planning to use data mining. *These departments and agencies reported 199 data mining efforts, of which 68 are planned and 131 are operational.* [emphasis added].

The figure here shows the most common uses of data mining efforts as described by agencies. Of these uses, the Department of Defense reported the largest number of efforts aimed at improving service or performance, managing human resources, and analyzing intelligence and detecting terrorist activities. The Department of Education reported the largest number of efforts aimed at detecting fraud, waste, and abuse. The National Aeronautics and Space Administration reported the largest number of efforts aimed at analyzing scientific and research information. For detecting criminal activities or patterns, however, efforts are spread relatively evenly among the agencies that reported having such efforts. *In addition, out of all 199 data mining efforts identified, 122 used personal information*. [emphasis added].

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses.* GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

3. William Arkin identifies over 500 “software tools, databases, data mining and processing efforts have been contracted for or are under development or in use at the NSA and other intelligence agencies and military commands today.”

Source: William Arkin. “NSA's Multi-Billion Dollar Data Mining Effort.” Washington Post May 12, 2006, http://blog.washingtonpost.com/earlywarning/2006/05/nsas_multibillion_dollar_data.html

4. The Federal Agency Data Mining Reporting Act of 2007 mandates that federal agencies must report their data mining to Congress.

Source: S.236, Federal Agency Data Mining Reporting Act of 2007, 110th Congress, 1st session, http://thomas.loc.gov

### Data Quality Act

Directed OMB (Office of Management and Budget) to issue, by Sept. 30, 2001, "policy and procedural guidance to Federal agencies" subject to the Paperwork Reduction Act (44 U.S.C. 35 & Public Law 106-554; H.R. 5658) requiring federal agencies to

- within one year of OMB's implementing guidelines, issue their own data quality guidelines "ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated";
- establish "administrative mechanisms allowing affected persons to seek and obtain correction of information maintained and disseminated by the agency that does not comply with the guidelines"
- report periodically to OMB once the guidelines are put in practice detailing "the number and nature" of data quality complaints received by the agency, as well as "how such complaints were handled.

Source: Susan M. Bisong. “Federal Agencies Subject to Data Quality Act.” http://library.findlaw.com/2003/Jan/14/132464.html and OMB Watch, http://www.ombwatch.org/article/archive/231?TopicID=2

### DCID 1/7, "Security Controls on the Dissemination of Intelligence Information”

1. Establishes policies, controls, procedures, and control markings for the dissemination and use of intelligence to ensure that it will be adequately protected.

Source: DoD. National Industrial Security Program Operating Manual (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

2. Directive establishes policies, controls, and procedures for the dissemination and use of intelligence information to ensure that, while facilitating its interchange for intelligence purposes, it will be adequately protected. This Directive implements and amplifies applicable portions of the directives of the Information Security Oversight Office issued pursuant to Executive Order 12958 (E.O.) and directives of the Security Policy Board issued pursuant to E.O. 12958 and PDD-29.

2.2 Additionally, this Directive sets forth policies and procedures governing the release of intelligence to contractors and consultants, foreign governments, international organizations or coalition partners consisting of sovereign states, and to foreign nationals and immigrant aliens, including those employed by the US Government.

2.3 Executive Order 12958 provides for the establishment of Special Access Programs, including Sensitive Compartmented Information. D.C.ID 3/29 provides procedures for the establishment and review of Special Access Programs pertaining to intelligence activities and restricted collateral information. Intelligence Community components may establish and maintain dissemination controls on such information as approved under the policies and procedures contained in D.C.ID 3/29, this D.C.ID, and implementing guidance.

Source: Director of Central Intelligence "Directive 1/7 Security Controls on the Dissemination of Intelligence Information." June 30, 1998, http://www.fas.org/irp/offdocs/D.C.id1-7.html

**DCS NET**

***See Altivore, CALEA, Carnivore***

The FBI's Digital Collection System Network, that can (allegedly) perform instant wiretaps on almost any communications device in the US.

Other systems:

DCS-3000 | DCS-3000 Network Map

DCS-5000

DCS-6000, known as Digital Storm, captures and collects the content of phone calls and text messages for full wiretap orders.

Source: EFF, FOIA Litigation, http://www.eff.org/fn/directory/3673/228 (serious redaction) and http://www.eff.org/issues/foia/061708CKK, Ryan Singel, "Point, Click…Eavesdrop." *Wired* August 2007, http://www.wired.com/politics/security/news/2007/08/wiretap

**Deception**

1. Those measures designed to mislead a foreign power, organization, or person by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.

Source: United States Intelligence Community, http://www.intelligence.gov/2-counterint_f.shtml

2. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests.

Source: DoD. *DoD Dictionary of Military and Associated Terms*. Joint Publication 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**Deception Means**

Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. physical means – Activities and resources used to convey or deny selected information to a foreign power. (Examples include military operations, including exercises, reconnaissance, training activities, and movement of forces; the use of dummy equipment and devices; tactics; bases, logistic actions, stockpiles, and repair activity; and test and evaluation activities); b. technical means – Military materiel resources and their associated operating techniques used to convey or deny selected information to a foreign power through the deliberate radiation, re-radiation, alteration, absorption, or reflection of energy; the emission or suppression of chemical or biological odors; and the emission or suppression of nuclear particles; c. administrative means – Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545-b.htm

**Declassification**

***See Automatic Declassification, Reclassification***

1. The determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

2. The process of reviewing and disclosing previously designated (classified) national security and nuclear related information classified by U.S. government branches, departments

and agencies. Executive Order 12356 [Reagan; 1982], Executive Order 12958 [Clinton; 1995] and Executive Order 13292 [Bush; 2003] set the stage for declassification.

EO12356 Sec. 3.3 "Systematic Review for Declassification" designated the Archivist of the United States (National Archives) to abide by the timeframes outlined by Information Security Oversight Office (ISOO). This EO set up a framework for affected agencies to review sensitive documents, specifically allowing declassification to take place within the originating agency.

EO12958 established a schedule beginning on October 17, 2001 for automatic declassification of historically valuable twenty-five year-old records that are not otherwise exempt. These records were to be automatically declassified after five years-the deadline came and went. EO13292 moved the 10/17/2001 schedule to December 31, 2006 and preserves 12958's Interagency Security Classification Appeals Panel (ISCAP), which has proven to be an exceptionally powerful tool for correcting classification abuses by subjecting them to the scrutiny of an interagency review panel. The new order would blunt the ISCAP's effectiveness, however, by permitting the Director of Central Intelligence to reject Panel rulings unless he is overridden by the President. (Section 5.3)

Source: Alvin S. Quist, http://www.fas.org/sgp/library/quist2/chap_11.html and *Secrecy News* March 13, 2003, http://www.fas.org/sgp/news/secrecy/2003/03/031303.html

3. Declassification means the authorized change in the status of information from classified information to unclassified information.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2

4. When a document is undergoing classification, a declassification date must be included. No declassification date entry is given for an unclassified document. ISOO directs the executive branch in its "orderly declassification" of historically valuable permanent classified records that are twenty-five years old or older. The deadline is December 31, 2006.

Source: ISOO *2004 Report to the President* http://www.archives.gov/isoo/reports/2004-annual-report.html and Steven Garfinkel." Senior Agency Officials of Entities Granted Original Classification Authority by the President." http://www.fas.org/sgp/isoo/suspdecl.html

5. Many of the nearly 260 million pages of classified national security information subject to automatic declassification by December 31, 2006, contain information of interest to other agencies. This means that the original agency must not only review the classified information for declassification, but it must then refer the document to any other agency that

has an interest in the classified information. While agencies have developed strategies to reduce the cost and time required, the referral of documents remains one of the most costly and lengthy components of the declassification review process. This is one reason why the recent amendment to the Order allowed agencies to delay the automatic declassification of classified records referred to them by other agencies for an additional three years. While classified records that fall into this category must be subject to automatic declassification until December 31, 2009. Based on the data provided, we estimate that 65 million pages (25 percent of the total) must be referred to and acted upon by other agencies by the extended date.

In addition to the 260 millions pages, 87 million pages of special media, such as motion pictures or audio tapes, (regardless of media we report volume in number of pages) will need to be declassified, exempted, or referred to other interested agencies by December 31, 2011, based upon the 5 additional years allotted by the recent amendment to the Order for information contained in special media.

Source: ISOO, Report to the President: An Assessment of Declassification in the Executive Branch, 2004 November 30, 2004, http://www.fas.org/sgp/isoo/2004declass.pdf

### Declassification Authority

(1) the official who authorized the original classification, if that official is still serving in the same position; (2) the originators current successor in function; (3) a supervisory official of either; or (4) officials delegated declassification authority in writing by the agency head or the senior agency official.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." Section 6.1(l), http://www.archives.gov/federal-register/executive-orders/2003.html and ISOO. "Frequently Asked Questions About E.O. 13292." http://www.archives.gov/isoo/faqs/eo-12958.html

### Declassification Event

An event that eliminates the need for continued classification of information.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

### Defense Central Index of Investigations

Reported 25 million index cards representing files on individuals and 760,000 cards representing files on organizations and incidents.

Source: United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Army Surveillance of Civilians: A Documentary Analysis*. 92nd Congress, second session. Washington, D.C.: U.S. Government Printing Office, 1972. 86.

**Defense Counterintelligence and Human Intelligence Center**

***See Counterintelligence Field Activity (CIFA)***

The DCHIC shall exercise administrative and management oversight of national security investigations (e.g., espionage) and related activities conducted by DoD CI organizations. DIA shall NOT be designated as a law enforcement activity and shall not perform any law enforcement functions previously assigned to DoD CIFA.

Source: DoD. Deputy Secretary for Defense, "Establishment of the Defense Counterintelligence and Human Intelligence Center (D.C.HC)," DTM 08-032, July 22, 2008, http://www.fas.org/irp/doddir/dod/D.C.hc.pdf

**Defense Critical Infrastructure Related Sensitive information**

Mentioned in DoD Directive 3020.40, but not defined.

Source: DoD. DoD Directive 3020.40. "Defense Critical Infrastructure Program (D.C.IP)," August 19, 2005, http://www.fas.org/irp/doddir/dod/d3020_40.pdf

**Defense Information**

1. Any document, writing, sketch, photograph, plan, model, specification, design prototype, or other recorded or oral information relating to any defense article, defense service , or major combatant vessel, but shall not include Restricted Data as defined by the Atomic Energy Act (AEA) of 1954, as amended, and data removed from the Restricted Data category under section 142 of that Act.

Source: Defense Acquisition University. *Glossary: Defense Acquisition Acronyms and Terms.* http://www.dau.mil/pubs/Glossary/preface.asp

2. Official information which requires protection in the interests of the national defense, which is not common knowledge, and which would be of intelligence value to an enemy or potential enemy in the planning or waging of war against the United States or its allies.

Source: Department of the Army Dictionary *of United States Army Terms*. Army Regulation 310-25. October, 1983, http://www.fas.org/irp/doddir/army/ar310-25.pdf

**Defense Information Infrastructure (DII)**
The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving Department of Defense (DOD) local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. Also called DII. See also global information infrastructure; information; infrastructure; national information infrastructure.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Defense Information Systems Network (DISN)**
Integrated network centrally managed and configured to provide long-haul information transfer services for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services. (JP 2-01)

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Defense Intelligence Production**
The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Defensive Counterinformation**
Actions protecting our military information functions from the adversary.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995. [See the Wayback Machine, http://web.archive.org/web/20040901091302/http://www.af.mil/lib/corner.html]

**Defensive Information Operations**

The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. See also counterintelligence; electronic warfare; information assurance; information operations; information system; offensive information operations; operations security; physical security; special information operations.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Defensive Information Warfare (IW-D)**

***See Cyberwar, Direct Information Warfare, Information Warfare, Netwar, Strategic Information Warfare***

All actions taken to defend against information attacks, that is, attacks on decision makers, the information and information-based processes they rely on, and their means of communicating their decisions. Strictly speaking, since these attacks can be launched during peace time at nonmilitary targets by nonmilitary groups, both foreign and domestic, the term IW-D should be IWS-D. However, IW-D is currently in wide use.

Source: David S. Alberts. *Defensive Information Warfare*. National Defense University Press Book, August 1996, http://tinyurl.com/ygf9xq9

**Degrade**

In information operations, using nonlethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems and information collection efforts or means.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Deliberate Compromise of Classified Information**

1. The act, attempt, or reported contemplation of intentionally conveying classified documents, information, or material to any unauthorized person, including unauthorized public disclosure. (18 USC 798).

Source: DoD. AR 381-12. January 15, 1993. "Subversion and Espionage Directed against the U.S. Army." http://fas.org/irp/doddir/army/ar381-12.pdf

2. 18 USC § 798 is actually titled "Disclosure of Classified information." [The word "deliberate" is not mentioned].

a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—
(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or (3) concerning the communication intelligence activities of the United States or any foreign government; or (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Source: 18 U.S.C.798. "Disclosure of Classified Information." http://www4.law.cornell.edu/uscode/

### Deny

In information operations, entails withholding information about Army force capabilities and intentions that adversaries need for effective and timely decisionmaking.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

### Deny In Toto

A category I recently discovered on a declassified document approved for release May 19, 1989. The document is titled "International Congress of Space Medicine," (Mexico, January 29, 1976) eight pages, heavily redacted, with blank pages labeled "Deny In Toto."

Source: DDRS (Declassified Documents Reference System), subscription database and microfiche available at academic libraries.

### Department of Defense Directive

A broad policy document containing what is required by legislation, the President, or the Secretary of Defense to initiate, govern, or regulate actions or conduct by the DoD Components within their specific areas of responsibilities. DoD Directives establish or describe policy, programs, and organizations; define missions; provide authority; and assign responsibilities. One-time tasking and assignments are not appropriate in DoD Directives.

Source: Department of Defense. Washington Headquarters. "DoD Issuances." http://www.dtic.mil/whs/directives/general.html

**Department of Defense Intelligence Information System (DODIS)**
The combination of Department of Defense personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national-level decision makers.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)**
***See Unclassified Information, Unclassified Controlled Nuclear Information***
Unclassified documents and material containing DoD UCNI shall be marked as follows:
(1) The face of the document and the outside of the back cover (if there is one) shall be marked "DoD Unclassified Controlled Nuclear Information."
(2) Portions of the document that contain DoD UCNI shall be marked with "(DoD UCNI)" at the beginning of the portion. b. Classified documents and material containing DoD UCNI shall be marked in accordance with Chapter V, except that:
(1) Pages with no classified information but containing DoD UCNI shall be marked "DoD Unclassified Controlled Nuclear Information" at the top and bottom.
(2) Portions of the document that contain DoD UCNI shall be marked with "(DoD UCNI)" at the beginning of the portion-in addition to the classification marking, where appropriate. c. Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings that alert the holder or viewer that the material contains DoD UCNI. d. Documents and material containing DoD UCNI and transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

DEPARTMENT OF DEFENSE
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION
EXEMPT FROM MANDATORY DISCLOSURE

(5 U.S.C. 552(b) (3), as authorized by 10 U.S.C. 128)

e. Transmittal documents that have DoD UCNI attachments shall bear a statement: "The attached document contains DoD Unclassified Controlled Nuclear Information (DoD UCNI)."

DoD. DOD 5200.1-R. "Information Security Program." Appendix C. January 1997, http://fas.org/irp/doddir/dod/5200-1r/appendix_c.htm

2. DoD Unclassified Controlled Nuclear Information (DoD UCNI) is unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities. Information is Designated DoD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities. Information may be designated DoD UCNI by the Heads of the DoD Components and individuals to whom they have delegated the authority.

Source: Office of the Secretary of Defense. 32 CFR 223, http://www.gpoaccess.gov/CFR/index.html.

**Department of State Sensitive But Unclassified**

Unclassified information that originated within the Department of State which warrants a degree of protection or administrative control and meets the criteria for exemption from mandatory public disclosure under FOIA. Prior to 26 January 1995, this information was designated and marked LOU [Limited Use Only]. The LOU designation will no longer be used.

Source: Centers for Disease Control. "Manual Guide - Information Security CD.C.-02."
Office of Security and Emergency Preparedness "Sensitive But Unclassified Information." 07/22/2005, http://www.fas.org/sgp/othergov/cD.C.-sbu.pdf.

**Derivative Classification**

1. Derivative classification is a determination that a document or material contains or reveals information already classified.

Source: Source: Arvin S. Quist. "Security Classification of Information." Chapter 1, http://www.fas.org/sgp/library/quist2/chap_1.html

2. A determination that information is in substance the same as information currently classified, and the application of classification markings.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

3. The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Derivative classifiers make 92% percent of all classification decisions.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended, http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and ISOO *2004 Report to the President* http://www.archives.gov/isoo/reports/2004-annual-report.html

4. Derivative classifiers may only classify documents or material when they have classification guidance in the form of a guide or classified source documents or other guidance by an original classifier.

Source: DOE. *Understanding Classification*. Washington, D.C.: U.S. Dept. of Energy, Assistant Secretary for Defense Programs, Office of Classification, 1987. SUDOC: E 1.15:0007/1

### Derogatory Information

1. Unfavorable information regarding an individual which brings into question the individuals' eligibility or continued eligibility for access authorization or suitability for federal employment. Specific types of derogatory information are listed in 10 CFR 710 (below) and Executive Order 10450.

Source: http://www.fas.org/irp/doddir/doe/o5631_2c/o5631_2ca2.htm, 59 FR 35185, July 8, 1994, as amended at 66 FR 47063, Sept. 11, 200, Energy. 10 CFR 710.8, http://www.gpoaccess.gov/CFR/index.html

### Direct Information Warfare

***See Cyberwar, Defensive Information Warfare, Information Warfare, Netwar, Strategic Information Warfare***

Changing the adversary's information without involving the intervening perceptive and analytical functions.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995., [See the Wayback Machine, http://web.archive.org/web/20040901091302/http://www.af.mil/lib/corner.html]

### Director of National Intelligence (DNI)

One of the recommendations of the National Commission on the Terrorist Attacks Upon the United States ("9/11 Commission") was to replace the position of the Director of Central Intelligence (D.C.I) with National Intelligence Director (NID) who would oversee and coordinate national intelligence agencies and programs.

The DNI coordinates the fifteen agencies that comprise the Intelligence Community (IC), and is the principal intelligence adviser to the president and the statutory intelligence advisor to the National Security Council. On April 21, 2005, authority was given under EO 12958 "Classified National Security Information," amended to classify up to Top Secret level.

Source: Alfred Cumming. "The Position of Director of National Intelligence: Issues for Congress." *CRS Report for Congress* August 12, 2004 http://www.fas.org/irp/crs/RL32506.pdf, "Designation Under Executive Order 12958" April 21, 2005, *Federal Register* April 26, 2005, http://www.fas.org/sgp/bush/wh042105.html, Office of the Director of National Intelligence http://www.dni.gov/ and Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("Silberman-Robb Commission"). March 31, 2005, http://www.gpoaccess.gov/wmd/index.html

### Disclosure

Disclosure means a transfer by any means of a record, a copy of a record, or the information contained in a record to a recipient other than the subject individual, or the review of a record by someone other than the subject individual.

Source: National Archives and Records Administration. 36 CFR 1202.4, http://www.gpoaccess.gov/CFR/index.html

### Discovery Process

A process controlled by a court, designed to compel the exchange of information before a trial. Discovery allows one party to question other parties, and sometimes witnesses; Discovery also allows one party to force the others to produce requested documents or other physical evidence. One major purpose of discovery is to assess the strength or weakness of an opponent's case, with the idea of opening settlement talks.

The most common types of discovery are interrogatories, which consist of written questions the other party must answer under penalty of perjury, and depositions, which involve an in-person

session at which one party to a lawsuit has the opportunity to ask oral questions of the other party or her witnesses under oath while a written transcript is made by a court reporter. Other types of pretrial discovery consist of written requests to produce documents and requests for admissions, by which one party asks the other to admit or deny key facts in the case.

Source: *Federal Rules of Civil Procedure* http://www.law.cornell.edu/rules/frcp/overview.htm and [Nolo] *Everybody's Legal Dictionary,* http://www.nolo.com/dictionary/dictionary_alpha.cfm?wordnumber=658&alpha=D

**Discretionary Access Control**

The means of restricting access to files based on the identity and need-to-know of users and/or groups to which the files belong.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

**Disinformation**

1. Carefully contrived misinformation prepared by an intelligence service for the purpose of misleading, deluding, disrupting, or undermining confidence in individuals, organizations, or governments.

Source: United States Intelligence Community, http://www.intelligence.gov/2-counterint_f.shtml

2. Information disseminated primarily by intelligence organizations or other covert agencies designed to distort information or deceive or influence US decisionmakers, US forces, coalition allies, key actors, or individuals via indirect or unconventional means.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

3. Misinformation that is deliberately disseminated in order to influence or confuse adversaries.

Source: Federal Geographic Data Committee. Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns." June 2005, http://www.fas.org/sgp/othergov/fgD.C.0605.pdf

4. Whereas Inaccurate information, distortions of truth, excessive limitations on access to information and the removal or destruction of information in the public domain are anathema to the ethos of librarianship and to the functioning of a healthy democracy; and

Whereas, Evidence exists revealing that some U.S. government officials and agencies use disinformation in pursuit of political and economic power, as well as war, thwarting the development of an informed citizenry and constituting a "critical problem facing society"; and

Whereas, The list of documented instances of government use of disinformation continues to grow, and includes:

- the distribution to media outlets of government produced "video news releases" under the guise of independent journalism;
- the use of commentators paid by government agencies to express views favorable to government policies in clear violation of Federal Communications Commission regulations;
- the censorship of scientific studies warning of the true threat of global warming;
- the fabrication and deliberate distortion of information used to justify the U.S. invasion of Iraq;
- the removal of public information from U.S. depository libraries; and
- heightened assaults on constitutional rights under the guise of "national security"

Source: American Library Association. "Resolution on Disinformation, Media Manipulation, and Destruction of Public Information." June 29, 2005, http://tinyurl.com/yfo34dg

5. So, disinformation is in the eye of the beholder, not necessarily a term that just has an agreed-on definition.

Source: Todd Leventhal, Chief of the Counter-Information Team, International Information Programs Bureau, U.S. Department of State, "Accuracy in the Media: Misinformation, Mistakes, and Misleading in American and Other Media," http://fpc.state.gov/fpc/44433.htm.

Soviet definitions:

1. From the Russian *dezinformatsia*, a division of the KGB devoted to black propaganda "false, incomplete, or misleading information that is passed, fed or confirmed to a targeted individual, group."

Source: Richard H. Shultz and Roy Godson. *Dezinformatsia:Active Measures in Soviet Strategy.* Washington: Pergamon-Brasey's, 1984.

2. *Dezinformatsionnyye svedeniya* (*dezinformatsiya*); disinformation specifically prepared information to give the enemy a false picture of events which might be used as a basis for decisions. Can be used to conceal state security agencies operational procedures, forces and resources, or deflecting an enemy towards a worthless target, etc.

3. *Dezinformatsionnyye operativnaya*: operational disinformation operational procedure which consists of providing the enemy with specific specially prepared information which will give a false picture of activity being undertaken by the counter-intelligence service and may encourage the enemy to take decisions which are advantageous to the counterintelligence service.

4. *Dezinformirovaniye* dissemination of information; Form of operational activity involving feeding disinformation to the enemy or to third parties in order to confuse them.

Source: Vasily Mitrokhin, ed. *KGB Lexicon: The Soviet Intelligence's Officer's Handbook*. London: Frank Cass, 2002.

**Disruptive Technology Office (DTO)**

***See Advanced Research Development Activity (ARDA)***

NSA's [National Security Agency] DTO fosters collaboration throughout the intelligence world with the technical and communities in academia, the national laboratories, and the commercial sector. DTO then helps transfer emerging solutions to the intelligence community technology centers for integration and implementation. Like DARPA, DTO also commonly uses broad area announcements. DTO funds geospatial sciences R&D jointly with NGA [national Geospatial Agency] through its Advanced Research in Interactive Visualization for Analysis (ARIVA) Program. DTO's mission is to sponsor high- risk, high-payoff research designed to leverage leading-edge technology in the solution of some of the most critical problems facing the IC. The phase one focus of DTO's ARIVA program seeks to dramatically improve the visualization of geospatially based national-level foreign intelligence information.

Source: Board on Earth Sciences and Resources. *Priorities for GEOINT Research at the National Geospatial-Intelligence Agency*. National Academies Press, 2006. 19. http://darwin.nap.edu/

**Disseminate**

An information management activity: to communicate relevant information of any kind from one person or place to another in a usable form by any means to improve understanding or to initiate or govern action.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Distribution Captions**

***See EXDIS, LIMDIS, NODIS STADIS***

1. Records bearing special distribution and channel captions require special handling and control, which is sometimes more restrictive than that required by their security classification alone. Detailed requirements for captions are contained in the Records Management Handbook, 5 FAH-4 H-213 [not online] and the Correspondence Handbook, 5 FAH-1 H700. [and 12 FAM 539].

Source: Department of State. *Foreign Affairs Manual*. 5 FAM 420, "Organizing, Maintaining, and Protecting Records." http://www.state.gov/m/a/dir/regs/

2. Wise (72) writes that captions were created under the Johnson Administration by then Executive Secretary of State Benjamin H. Read.

Source: David Wise. *Politics of Lying: Government Deception, Secrecy, and Power*. New York, Random House 1973.

**Dissent Channel**

The Dissent Channel is reserved for consideration of dissenting or alternative views on substantive foreign policy matters. The Dissent Channel may not be used to address non-policy issue. Complaints relating to violation of law, rules, or regulations; mismanagement; or fraud, waste, or abuse may be addressed to OIG/INV (see 1 FAM 053 paragraph c). Classification challenges should not be addressed through the Dissent Channel (see subpart C or 22 CFR 171).

Source: U.S. Department of State. *Foreign Affairs Manual*. 2FAM070, "Dissent Channel." (F2AM071.2), http://www.state.gov/m/a/dir/regs/

**Document and Material**

1. Any recorded information, regardless of the nature of the medium or circumstances of the recording.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information."
http://www.archives.gov/federal-register/executive-orders/2003.html

2. Any recorded information, regardless of its physical form or characteristics, without limitation, written or printed matter, automated data processing storage media, maps, charts,

paintings, drawings, films, photographs, imagery, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

### Document and Page Markings

*See Classification Markings / Control Markings*

If a document contains some Secret information and some Confidential information, the overall marking would be "Secret." This marking must be placed at the top and bottom of the outside of the front cover (if any), the title page (if any), on the first page, and on the outside of the back cover (if any). Interior pages of classified documents must also be marked.

Source: Defense Intelligence Agency. Office of Security and Counterintelligence, Policy and Security Awareness Branch. *Desk Reference Guide to Executive Order 12958, as Amended, Classified National Security Information.* April 2004.

### Document Exploitation (DOCEX)

The systematic extraction of information from documents either produced by the threat, having been in the possession of the threat, or that are directly related to the current or future threat situation for the purpose of producing intelligence or answering information requirements. This may be conducted in conjunction with human intelligence (HUMINT) collection activities or may be conducted as a separate activity.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

### DOJ Media Leak Questionnaire

E4.1.1. If the media discloses classified information without proper authorization, the Heads of the DoD Components shall submit the DOJ Media Leak Questionnaire through security channels to the USD (I). In coordination with the DoD GC, the USD(I) shall prepare a letter addressed to the attention of Chief, Internal Security Section, Criminal Division, Bond Building, Room 9400, U.S. Department of Justice, 1400 New York Avenue, Northwest, Washington, D.C.

Source: DoD Directive 5210.50, July 22, 2005, http://www.dtic.mil/whs/directives/corres/pdf/521050p.pdf

## Do Not File

1. J. Edgar Hoover necessitated the creation of written records, which might need to be produced in response to a congressional subpoena or court-ordered discovery motion. Hoover minimized this risk through a Do Not File procedure. Documents captioned "Do Not File" were not to be indexed in the FBI's central records system but instead were to be routed to the office files of senior FBI officials at the FBI's Washington, D.C., headquarters for review and approval (and were then to be regularly destroyed). The head of an FBI field office, in turn, created an "informal" memorandum (that is, a nonofficial record) of each authorization and filed it in the office safe "until the next inspection by Bureau Inspectors, at which time it [the informal memo] is destroyed" (see Exhibit 5.7, pages 184–86). The Do Not File procedure refined another special records procedure that Hoover had devised in 1940 to safeguard sensitive communications among senior FBI officials. To distinguish these more sensitive informal memoranda from official memoranda that were to be serialized and indexed in the FBI's central records system, an informal memorandum was to be written on pink paper (official memoranda were written on white paper) and to contain the notation that the memorandum was "to be destroyed after action is taken and not sent to files."

Dating from their inception as a special recordkeeping method, informal and Do Not File memoranda were to be destroyed "after action is taken." FBI assistant directors retained these memoranda in their office files and decided when to destroy them. In March 1953, Hoover ended this discretionary arrangement and ordered FBI assistant directors to "destroy them as promptly as possible but in no case shall they be retained in excess of six months."

Source: Athan Theoharis, ed. *The FBI: A Comprehensive Reference Guide*. Phoenix: Oryx Press, 1998. 22, 32, 183–86,366, 376.

2. The Do Not File procedure was not a unique FBI practice for sanitizing the record.

Source: Athan Theoharis. "Secrecy and Power: Unanticipated Problems in Researching FBI Files. *Political Science Quarterly* 119 no.2 (2004): 271–290.

## Dossier

An official file of investigative, intelligence, or ci materials collected on behalf of the U.S. Army. May consist of documents, film, magnetic tape, photographs, or a combination thereof. May be "personal" referring to an individual or "impersonal" referring to a thing, event or organization.

Source: DoD. Army Regulation AR381-45. "Investigative Records Repository." August 25, 1989, http://www.army.mil/usapa/epubs/pdf/r381_45.pdf

## DOSTN (Department of State Telecommunications Network)

A "black" transmission facility.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/

**Downgrading**

1. A determination made by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

2. Changing a security classification from a higher to a lower level.

Source: National Imagery and Mapping Agency. *NIMA Guide to Marking Classified Documents*, October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

**Drug Enforcement Administration Sensitive Information**

***See Classification Markings / Control Markings, Unclassified Information***

DEA Sensitive information is unclassified information that is originated by the Drug Enforcement Administration and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. The Administrator and certain other officials of the DEA have been authorized to designate information as DEA Sensitive; the Department of Defense has agreed to implement protective measures for DEA Sensitive information in its possession. Types of information to be protected include:

a. Information and material that is investigative in nature;
b. Information and material to which access is restricted by law;
c. Information and material that is critical to the operation and mission of the DEA; and
d. Information and material the disclosure of which would violate a privileged relationship.

Access to DEA Sensitive information shall be granted only to persons who have a valid need-to-know for the information. A security clearance is not required. DEA Sensitive information in the possession of the Department of Defense may not be released outside the Department without authorization by the DEA.

Source: DoD. DOD 5200.1-R Information Security Program. Appendix C, http://fas.org/irp/doddir/dod/5200-1r/appendix_c.htm

**Drug/Financial Fusion Center**

***See Data Mining, Fusion Centers***

Department of Justice Headquarters. Will contain data from, and be used by, Organized Crime and Drug Enforcement Task Force agencies. The system will permit the collection and cross case analysis of all drug and related financial investigative data;
Purpose: Detecting criminal activities or patterns;
Status: Planned;
Features: Personal information: Yes;
Features: Private sector data: Yes;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Dual Use (Information)**

Items that have both commercial and military or proliferation applications. While this term is used informally to describe items that are subject to the EAR, purely commercial items are also subject to the EAR (see Sec. 734.2(a) of the EAR).

Source: Terms used in Export Administration Regulations (EAR) 15 CFR 772.1, http://www.gpoaccess.gov/cfr/index.html

**Dysfunctional Information Restrictions**

A great deal of information restriction is legacy, stemming from the felt need to guard military-related information from disclosure to those who can harm us. A more limited quantity of information may be restricted in the interests of efficiency of government. To accommodate that interest, the Congress, in enacting the Freedom of Information Act, permitted exemption from mandatory disclosure of pre-decisional advice to decision-makers, data relevant to criminal investigations and information of so minor a nature as to not merit the effort to retrieve and disclose it. Other data has been predetermined by Congress to merit withholding. This might include nuclear energy-related information, information about the personnel and processes of intelligence organizations or personal privacy information.

Source: M.E. Bowman, "Dysfunctional Information Restrictions" by M.E. Bowman, *Intelligencer: Journal of U.S. Intelligence Studies* Fall/Winter 2006-2007, http://www.fas.org/sgp/eprint/bowman.pdf

## ~ E ~

### Eagle Eyes

The Eagle Eyes program is an Air Force anti-terrorism initiative that enlists the eyes and ears of Air Force members and citizens in the war on terror. Eagle eyes teaches people about the typical activities terrorists engage in to plan their attacks. Armed with this information, anyone can recognize elements of potential terror planning when they see it. The program provides a network of local, 24-hour phone numbers to call whenever a suspicious activity is observed. You and your family are encouraged to learn the categories of suspicious behavior and stay attuned to your surroundings. If you observe something suspicious, send your input using this "Crimebusters" link, or alert local authorities.

Source: Air Force Office of Special Investigations, http://www.osi.andrews.af.mil/eagleeyes/index.asp

### Early Report

A seven to nine page document based on reporting of editorial commentary from major posts commenting on the issues of the day. It is electronically transmitted to high level officials at the White House, State Department, Pentagon and other senior affairs decision makers by 8:00 a.m. Monday through Friday.

Source: Department of State. *Foreign Affairs Manual*. 10 FAM 413.2, "Office of Research." http://www.state.gov/m/a/dir/regs/

### Earmark

1. An earmark is a line-item that is inserted into a bill to direct funds to a specific project or recipient without any public hearing or review. Members of Congress—both in the House and the Senate—use earmarks to direct funds to projects of their choice. Typically earmarks fund projects in the district of the House member or the state of the Senator who inserted it; the beneficiary of the funds can be a state or local agency or a private entity; often, the ultimate beneficiary is a political supporter of the legislator.

Source: Sunlight Foundation. "Earmark FAQ." http://www.sunlightfoundation.com/earmarksFAQ

2. A *Wall Street Journal* column on March 26 (2008) reported that the Congressional Research Service "will no longer respond to requests from members of Congress on the size, number of background of [budget] earmarks." The new CRS policy, the *Journal* article alleged, "is helping its masters hide wasteful spending."

Source: FAS has included both the *Wall Street Journal* and CRS' response here:

http://www.fas.org/sgp/crs/crs032607.pdf

**ECHELON**

Associated with a global network of computers that automatically search through millions of intercepted messages for pre-programmed keywords or fax, telex and e-mail addresses. Every word of every message in the frequencies and channels selected at a station is automatically searched. The processors in the network are known as the ECHELON Dictionaries. ECHELON connects all these computers and allows the individual stations to function as distributed elements an integrated system. An ECHELON station's Dictionary contains not only its parent agency's chosen keywords, but also lists for each of the other four agencies in the UK-USA system [NSA, GCHQ, DSD, GCSB and CSE]

Source: FAS. http://www.fas.org/irp/program/process/echelon.htm ; Temporary Committee on the ECHELON Interception System. http://www.europarl.eu.int/committees/echelon_home.htm ; Constant Brand. "Europeans Warned over Echelon Spying." *The Guardian* May 2001, http://www.guardian.co.uk/europarl/Story/0,2763,498440,00.html

**Effect of Failure to Publish**

Provides that, except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or to be adversely affected by, a matter required to be published in the *Federal Register* and not so published.

Source: "Public Information." 5 U.S.C. 552(a) (1), http://www.gpoaccess.gov/uscode/browse.html

**Electromagnetic Deception**

The deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are: a. manipulative electromagnetic deception—Actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces; b. simulative electromagnetic deception—Actions to simulate friendly, notional, or actual capabilities to mislead hostile forces; c. imitative electromagnetic deception—The introduction of electromagnetic energy into enemy systems that imitates enemy emissions.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Electronic Self-Disclosure**

EPA's Web-based system allows for electronic self-disclosure under the EPA Audit Policy. The pilot program, known as the Audit Policy Self-Disclosure system or eDisclosure, allows companies nationwide to electronically self-disclose violations of the Emergency Planning and Community Right-to-Know Act (EPCRA) including:

- Emergency Notification (section 304)
- CERCLA section 103 (only if Emergency Notification violation disclosed)
- Material Safety Data Sheets (section 311)
- Emergency and Hazardous Chemical Inventory Forms (section 312)
- Toxic Chemical Release Forms (section 313)

A business confidentiality claim may not be asserted with respect to any information submitted through eDisclosure.

Source: EPA, http://www.epa.gov/compliance/incentives/auditing/edisclosure.html

**Electronic Surveillance Statistics**

***See Communications Assistance for Law Enforcement Act***

The Omnibus Crime Control and Safe Streets Act of 1968 requires the Administrative Office of the United States Courts (AO) to report to Congress the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral, or electronic communications. The Wiretap Report covers intercepts concluded during each calendar year, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

Source: CALEA Implementation Unit (CIU), Electronic Surveillance Technology Section, Operational Technology Division, Federal Bureau of Investigation. http://www.askcalea.net/faqs.html#18 and U.S. Courts. *Wiretap Report* , http://www.uscourts.gov/library/wiretap.html

**Electronic Warfare (EW)**

***See Information Operations***

Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack.

Source: DoD. *Information Operations*. JP 3-13, February 13 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

**Elicitation**

Acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation. A technique of human source intelligence collection, generally overt, unless the collector is other than he or she purports to be.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**ELSUR File**

In September 1966, Assistant Attorney General Fred Vinson orders the creation of a special ELSUR Index to record the names of all individuals whose conversations had been intercepted by FBI wiretaps or bugs. An FBI term; an ELSUR file is the recording of all authorized wiretaps.

Source: Athan Theoharis, ed. *The FBI: A Comprehensive Reference Guide*. Phoenix: Oryx Press, 1998. 77, 372.

**Environmental Document**

***See Environmental Impact Statement***

Includes the documents specified in Sec. 1508.9 (environmental assessment), Sec. 1508.11 (environmental impact statement), Sec. 1508.13 (finding of no significant impact), and Sec. 1508.22 (notice of intent).

Source: 40 CFR 1508.10. "Definitions." http://www.gpoaccess.gov/cfr/index.html

**Environmental Impact Statement (EIS)**

***See State Secrets Privilege***

1. A detailed written statement as required by section 102(2) (C) of the Act.

Source: 40 CFR 1508.11. "Definitions." http://www.gpoaccess.gov/cfr/index.html

2. (C) include in every recommendtion or report on proposals for legislation and other major Federal actions significantly affecting the quality of the human environment, a detailed statement by the responsible official on --

(i) the environmental impact of the proposed action, (ii) any adverse environmental effects which cannot be avoided should the proposal be implemented, (iii) alternatives to the proposed action, (iv) the relationship between local short-term uses of man's environment and the maintenance and enhancement of long-term productivity, and (v) any irreversible and

irretrievable commitments of resources which would be involved in the proposed action should it be implemented.

Source: National Environmental Policy Act of 1969 (Pub. L. 91-190, 42 U.S.C. 4321-4347 , or "NEPA"), http://ceq.eh.doe.gov/nepa/regs/nepa/nepaeqia.htm

3. NEPA section 102(2)(C) calls for each Environmental Impact Statement (EIS), along with comments received from various federal, state, and local agencies, to be made available to the public "as provided by section 552 of Title 5." This statutory cross-reference is to the Freedom of Information Act (FOIA) which exempts properly classified agency records from public disclosure. CEQ regulations implementing NEPA allow the attachment of sensitive data to an EIS as a classified appendix, making the data available to members of Congress and agency officials with proper security clearances. Therefore, a court confronted with a NEPA enforcement case in which an EIS contains classified information must first ask whether the information could properly be withheld from a FOIA requester.

Source: Stephen Dycus. "NEPA Secrets." *New York University Law Journal* 2 no. 2 (1993), http://www1.law.nyu.edu/journals/envtllaw/issues/vol2/2/2nyuelj300.html

**Equity**

***See Original Classification Authority (OCA)***

Information originally classified by or under the control of an agency.

Source: National Defense. "Classified National Security Information." 32 CFR 2001, http://www.gpoaccess.gov/CFR/index.html

**Espionage**

1. The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation.

Source: DoD. AR 381-12. January 15, 1993. "Subversion and Espionage Directed against the U.S. Army." http://fas.org/irp/doddir/army/ar381-12.pdf,
Harold Edgar and Benno C. Schmidt, Jr. "The Espionage Statutes and Publication of Defense Information." *Columbia Law Review* 73 (1973): 929-1087, 18 U.S.C 793 http://assembler.law.cornell.edu/uscode/; Article 106a, *Uniform Code of Military Justice,* http://www4.law.cornell.edu/uscode/html/uscode10/usc_sup_01_10.html and Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, December 2006, http://www.firstamendmentcenter.org/about.aspx?id=18048

2. The Foreign Intelligence Surveillance Act (FISA) can be used to monitor U.S. persons who engage in unlawful collection of classified or controlled information even if they are not acting on behalf of a foreign power. That is the upshot of an August 14 ruling (pdf) disclosed last week in the case of two former officials of the American Israel Public Affairs Committee (AIPAC).The defendants had argued that they were improperly subjected to FISA surveillance since FISA requires that the target be "an agent of a foreign power" and, they insist, they were never acting on behalf of a foreign power.

Source: FAS. "FISA Surveillance Can Target Non-Spies." *Secrecy News* August 28, 2006 and OMB Watch. "New Official Secrets Law?: Case Threatens Open Government and Freedom of Press." August 22, 2006, http://www.ombwatch.org/article/articleview/3566/1/459?TopicID=2

**Essential Elements of Friendly Information (EEFI)**
Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. Also called EEFI.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Essential Elements of Information (EEIs)**
The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision.

Source: Department of Defense. *DoD of Military and Associated Terms. Amended*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Estimative Intelligence**
A category of intelligence analysis which judgments are made despite incomplete information. There are two basic types: What is going on? and What will happen?

Source: Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C.: Springfield, VA: National Technical Information Service, [1999?]. SUDOC: PREX 3.2:C 76 and PREX 3.2/2:G 94

**Estimative Language**
What We Mean When We Say: An Explanation of Estimative Language
When we use words such as "we judge" or "we assess"—terms we use synonymously—as well as "we estimate," "likely" or "indicate," we are trying to convey an analytical assessment or

judgment. These assessments, which are based on incomplete or at times fragmentary information are not a fact, proof, or knowledge. Some analytical judgments are based directly on collected information; others rest on previous judgments, which serve as building blocks. In either type of judgment, we do not have "evidence" that shows something to be a fact or that definitively links two items or issues.

Source: Office of the Director of National Intelligence, *Prospects for Iraq's Stability: A Challenging Road Ahead* January 2007, http://www.dni.gov/nic/PDF_GIF_otherprod/Iraq_NIE_Key_Judgments.pdf

**Evidential Value**
The usefulness of records in documenting the organization, functions, and activities of the agency creating or receiving them. Considered by NARA in appraising records for permanent retention.

Source: DOE. Chief Information Officer. "Records Management Definitions." http://cio.energy.gov/rmdefinitions.pdf

**Execution Information**
Information that communicates a decision and directs, initiates, or governs action, conduct, or procedure.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Executive Order (EO)**
1. Executive orders are official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

The text of Executive Orders appears in the daily *Federal Register* as each Executive Order is signed by the President, and received by the Office of the Federal Register. The text of Executive Orders beginning with Executive Order 7316 of March 13, 1936, also appears in the sequential editions of Title 3 of the *Code of Federal Regulations* (CFR).

Source: National Archives and Records Administration (NARA). "Executive Order FAQ's." http://www.archives.gov/federal-register/executive-orders/about.html

2. The Presidential system of information restriction that grew out of World War Two became an "extravagant and indefensible system of denial" exercised by the Executive Branch that had no "standing in law" (Schlesinger 341). Arthur Schlesinger (360) says

> …secrecy by definition meant that policies undertaken without consent. It would therefore be in the interest of Presidents to reopen the Presidency. But recent Presidents either have become so enamored of the short-run conveniences of secrecy, or else had enough to conceal, they forgot the long-run necessity, above all for the Presidency itself, of open government.

Source: Arthur Schlesinger. *The Imperial Presidency*. New York: Atlantic Monthly, 1973.

3. The President's authority to issue executive orders derives from powers both enumerated, implied and inferred by the Constitution, as well as from authority delegated to the President by Federal statute.

In the overwhelming majority of cases, executive orders and proclamations are an appropriate public way of guiding the actions of numerous Federal agencies and other components of the Executive branch. While thousands of executive orders have been issued over the last two centuries, Federal courts have been extremely reluctant to challenge executive authority. When executive orders are issued without a constitutional or legal basis, they implicate the Separation of Powers Doctrine that underpins divided government.

Source: Congressman Bob Barr, *Executive Orders and Presidential Directives*. Hearing before the Subcommittee on Commercial and Administrative Law of the Committee on the Judiciary, House of Representatives, One Hundred Seventh Congress, first session, March 22, 2001, http://commdocs.house.gov/committees/judiciary/hju72142.000/hju72142_0.htm

4. "Stroke of the pen. Law of the Land. Kinda cool."

Source: Paul Begala, (former Clinton Administration advisor). *New York Times*, July 5, 1998.

**Exempted**

***See Freedom of Information Act Exemptions***

Nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification under Executive Order 12958 "Classified National Security Information," amended.

Source: National Defense. "Classified National Security Information." 32 CFR 2001, http://www.gpoaccess.gov/CFR/index.html.

**Exemptions**

***See Freedom of Information Act Exemptions, Presidential Restrictions***

Statutory, regulatory and administrative designations that restrict public disclosure of information due to privacy and confidentiality issues, trade secrets, proprietary, export controls, law enforcement, homeland or national security concerns.

Categories of records exempt from disclosure under 5 U.S.C. 552.
:
Source: "Public Information." 5 U.S.C. 552. http://www.gpoaccess.gov/uscode/browse.html; also see Freedom of Information Act Guide, March 2007, http://www.usdoj.gov/oip/foia_guide07.htm

**Exercise Term**

***See Code Word | Codeword, NICKA, Nickname***

A nickname or code word, normally an unclassified nickname, used to designate a test, drill or exercise. An exercise term is employed to prevent confusion between exercise directions and actual operations.

Source: Chairman of the Joint Chiefs of Staff Manual. *Code Word, Nickname and Exercise Term Report (Short Title – NICKA)* April 1998, http://fas.org/irp/doddir/dod/cjcsm3150_29a.pdf

**Exformation**

Explicitly discarded information…what we call information in everyday life is really more like Exformation: in everyday language if something contains information, it is a result of the production of Exformation; it is a summary, an abbreviation suitable for guiding a transaction (108). Exformation is perpendicular to information (95). What is rejected before expression; it is about the mental work we do to probe what we want say.

Source: Tor Nørretranders. *The User Illusion: Cutting Consciousness Down to Size*. Trans.Jonathan Sydenham.New York: Viking Penguin, 1998.

**Exigent Letters**

Prior to enactment of the ECPA [Electronic Communications Privacy Act], the Supreme Court held that customers had no Fourth Amendment protected privacy rights in the records the telephone company maintained relating to their telephone use. Where a recognized expectation of privacy exists for Fourth Amendment purposes, the Amendment's usual demands such as those of probable cause, particularity, and a warrant may be eased in the face of exigent circumstances. For example, the Fourth Amendment requirement that officers must knock and announce their purpose before forcibly entering a building to execute a warrant can be eased in the presence of certain exigent circumstances such as the threat of the destruction of evidence

or danger to the officers. Satisfying Fourth Amendment requirements, however, does not necessary satisfy statutory demands.

The ECPA prohibits communications service providers from supplying information concerning customer records unless one of the statutory exceptions applies. There are specific exceptions for disclosure upon receipt of a grand jury subpoena89 or an NSL. A service provider who knowingly or intentionally violates the prohibition is subject to civil liability, but there are no criminal penalties for the breach.

Source: Source: Charles Doyle, "National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments," *CRS Report to Congress* September 8, 2009, RS22406 http://www.fas.org/sgp/crs/intel/RS22406.pdf

### Exploit

In information operations, to gain access to adversary command and control systems to collect information or to plant false or misleading information.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

### Exploitable Resources

Formulae, designs, drawings, research data, computer programs, technical data packages, and the like, which are not considered records within the Congressional intent of reference because of development costs, utilization, or value. These items are considered exploitable resources to be utilized in the best interest of all the public and are not preserved for informational value or as evidence of agency functions. Requests for copies of such material shall be evaluated in accordance with policies expressly directed to the appropriate dissemination or use of these resources. Requests to inspect this material to determine its content for informational purposes shall normally be granted, unless inspection is inconsistent with the obligation to protect the property value of the material, as, for example, may be true for patent information and certain formulae, or is inconsistent with another significant and legitimate governmental purpose.

Source: Federal Emergency Management Agency (FEMA), Department of Homeland Security. "Production or Disclosure of Information." 44 CFR 5.3, http://www.gpoaccess.gov/cfr/index.html

### Exploitation

DoD and NATO term: 1. (DOD only) Taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already achieved. 2.

Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. 3. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Export Controlled Information**

1. Information and technology that may only be released to foreign nationals or foreign persons in accordance with the Export Administration Regulations (15 CFR parts 730-774) and the International Traffic in Arms Regulations (22 CFR parts 120-130), respectively. Export controls regulate the transfer of certain information and potential equipment to foreign nationals, and "therefore constrain who can participate in associated research and educational activities."

Source: *Federal Register* July 12, 2005 (Volume 70, Number 132). http://www.gpoaccess.gov/fr/index.html and Center for Strategic and International Studies (CSIS) "Security Controls on Scientific Information and the Conduct of Scientific Research." http://www.csis.org/index.php?option=com_csis_pubs&task=view&id=32

2. Export controlled information or material is information or material that cannot be released to foreign nationals or representatives of a foreign entity without first obtaining approval or license from the Department of State. This pertains to items controlled by the International Traffic in Arms Regulations or the Department of Commerce and includes items controlled by the Export Administration Regulations. Export controlled information must be controlled as SBU information and marked accordingly.

Source: Centers for Disease Control. "Sensitive But Unclassified Information." February 2006, http://www.fas.org/sgp/othergov/cD.C.-sbu-2006.html

**Extraordinary Security Measures**

***See Code words / Codewords, Nickname, Sensitive Compartmented Information (SCI) Control Systems/Codewords, Special Access Program***

A security measure necessary to adequately protect particularly sensitive information but which imposes a substantial impediment to normal staff management and oversight. Extraordinary security measures are -

a. Program access nondisclosure agreements (read-on statements).
b. Specific officials authorized to determine "need-to-know" (ACA/access approval authority).
c. Nicknames/codewords for program identification.

d. Special access required markings.
e. Program billet structure.
f. Access roster.
g. Use of cover.
h. Use of special mission funds or procedures.
i. Use of a SAP facility/vault.
j. Use of a dedicated SAP security manager.
k. Any other security measure beyond those required to protect collateral.
l. Information in accordance with AR 38-5.

Source: Department of the Army. "Special Access Programs (SAPs) and Sensitive Activities." AR 380-381. April 21, 2004, http://www.fas.org/irp/doddir/army/ar380-381.pdf

**Extremely Sensitive Information**

1. Information and material related to the Single Integrated Operational Plan (SIOP) for the conduct of nuclear war fighting operations.

Source: John Pike, "Security and Classification." http://www.ostgate.com/classification.html

2. [Loosely defined] manufacturing details; R & D information.

Source: Ira S. Winkler. "Anatomy of an Industrial Espionage Attack." Defense Security Services. [See the Wayback Machine, http://tinyurl.com/ya8ccr6 ]

---

**~ F ~**

**Fabricator**

Individuals or groups who, without genuine resources, invent information or inflate or embroider over news for personal gain or for political purposes.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Fair Information Principles**

Collection Limitation Principle
Data Quality Principle
Purpose Specification Principle
Use Limitation Principle

Security Safeguards Principle
Openness Principle
Individual Participation Principle
Accountability Principle

Source: Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris, 1980)

**Fake News**
***See Information Blowback, Information Laundering, Prepackaged News***

**FBI Central Records System Classifications**
For a list of Records System Numbers, see Michael J. Ravnitzky's helpful list at http://www.newstrench.com/03secret/0categories.html; the FBI's *Conducting Research in FBI Records,* 8th edition, 1994; the FBI research page at http://www.fbi.gov/research.htm; Athan G. Theoharis, "Secrecy and Power: Unanticipated Problems in Researching FBI Files." *Political Science Quarterly* 119 no.2 (2004): 271-290, and his *FBI: An Annotated Bibliography and Research Guide.* New York: Garland, 1994.

**FBI Biometric Center of Excellence**
Leveraging the FBI's extensive experience in biometrics, this program is committed to strengthening criminal investigations and enhancing national security, while protecting the privacy rights of individuals.

Source: FBI, BCOE, http://www.biometriccoe.gov/About.htm

**FBI Intelligence Community Data Marts**
***See Data Mining***
Federal Bureau of Investigation. Is intended to take a subset of approved data from a data warehouse and make it available to the intelligence community;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Planned;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. Data Mining: Federal Efforts Cover a Wide Range of Uses. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Federal Agency Media Policies**

***See Prepublication Review***

To assess the degree of freedom with which science is communicated at federal agencies, the Union of Concerned Scientists conducted an investigation of 15 federal regulatory and science agencies. First, we analyzed existing policies governing communication with the media and the public. Second, we surveyed a cross-section of federal scientists to assess how these policies are put into practice.

**What We Found**

Both good policy and good practice in the communication of scientific results to the media are achievable goals for federal agencies. Yet there is no consistency among agency policies, and the ability of government scientists to speak freely about their research depends on the agency that employs them.

Source: UCCS, Freedom to Speak: A Report Card on Federal Media Policies, http://www.ucsusa.org/assets/documents/scientific_integrity/Freedom-to-Speak.pdf

**Federal Information Resources Management Regulations (FIRMR)**

Regulations on information resources management issued by GSA and applicable to Federal agencies.

Source: DOE. Chief Information Officer. "Records Management Definitions." http://cio.energy.gov/rmdefinitions.pdf

**Federal Register**

The 1935 Federal Register Act created the daily publication the *Federal Register*. Since Saturday, March 14, 1936, each daily issue of the Federal Register has published, in order: (1) Presidential documents, such as proclamations and executive orders; (2) federal agency rules and regulations; (3) Proposed rules; (4) Notices; and (5) Notices of Sunshine Act meetings. The *Federal Register* also contains proposed, interim and final rules. Most proposed rules are published first as proposals, with an invitation for public comment and review, before rules become final and have the force of law. Interim and final rules have the force of law.

Source: National Archives and Records Administration, http://www.archives.gov/federal-register/laws/federal-register and 44 U.S.C. Chapter 15. http://www.gpoaccess.gov/uscode/index.html

**Feedback**

In information operations, information that reveals how the deception target is responding to the deception story and if the military deception plan is working.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Field Manual**

A manual containing instructional, informational, and reference material relative to military training and operations. It is the primary means of promulgating military doctrine, tactics, and techniques.

Source: Department of the Army Dictionary *of United States Army Terms*. Army Regulation 310-25. October, 1983, http://www.fas.org/irp/doddir/army/ar310-25.pdf

**Field Press Censorship**

***See Censorship***

The security review of news material subject to the jurisdiction of the Armed Forces of the United States, including all information or material intended for dissemination to the public. Also called FPC.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**File Mystique**

Indeed, the history of private intelligence institutions in this country may be charted by tracing the accumulation and transfer of file collections. Maintaining a file collection on a particular subject serves two purposes: (1) the collection and consolidation of material in order to maximize the subversive character of the subject, whether an individual or an organization ; and (2) identification for aggressive purposes, the compilation of an "enemies list" for adverse present action, and as targets in the eschatological politics of deferred reckoning. The filing imperatively reflects the deep rooted conviction that the enemy is a conspiracy of real people, cunning deceivers who must first be first be identified, then cornered, and ultimately destroyed. The mere act of opening a countersubversive file on a subject is an exercise of power, an outlet for hostile emotion and intention. File work also has an objective, political dimension. It fortifies the resistance to change by linking it to governmental overthrow and social disruption. In this respect it distills the essentially negative quality of American conservatism, which typically seeks to generate political energy by attacking measures that threaten the status quo without submitting its own premises to the test of the democratic process.

Source: Frank Donner. *The Age of Surveillance*. New York: Knopf, 1980. 416.

**Files**

An arrangement of records. The term is used to denote papers, photographs, photographic copies, maps, machine-readable information, or other recorded information regardless of physical form or characteristics, accumulated or maintained in filing equipment, boxes, or machine-readable media, or on shelves, and occupying office or storage space.

Source: National Archives and Records Administration. 36 CFR 1220 "Federal Records, General." http://www.gpoaccess.gov/cfr/index.html

**File Series**

***See Integral File Block***

File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended, http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

**Finished Intelligence (FI)**

Raw information analyzed and corroborated. It should be produced in a consistent format to enhance utility and regularly disseminated to a defined audience.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004. http://www.cops.usdoj.gov/default.asp?Item=1404

**FIRSTFRUITS Database**

The journalist surveillance program, code named "Firstfruits," was part of a Director of Central Intelligence (DCI) program that was maintained at least until October 2004 and was authorized by then-DCI Porter Goss. Firstfruits was authorized as part of a D.C.I "Countering Denial and Deception" program responsible to an entity known as the Foreign Denial and Deception Committee (FDDC).

The organization partly involved in directing the National Security Agency program to collect intelligence on journalists -- Firstfruits -- is the Foreign Denial and Deception Committee (FDDC), a component of the National Intelligence Council. Firstfruits particularly targeted State Department and CIA insiders who were leaking information about the "cooking" of pre-war

WMD intelligence to particular journalists, including those at the *New York Times*, *Washington Post*, and CBS *60 Minutes*.

Source: Sourcewatch, http://www.sourcewatch.org/index.php?title=Firstfruits

**FOIA Request**

***See Exemptions, Freedom of Information Act, Freedom of Information Act Exemptions, Presidential Restrictions***

1. A written request for access to records of the executive branch of the Federal Government held by NARA, including NARA operational records, or to Presidential records in the custody of NARA that were created after January 19, 1981, that cites the Freedom of Information Act.

Source: National Archives and Records Administration. 36 CFR 1250.2, http://www.gpoaccess.gov/CFR/index.html

2. A FOIA request can be made for any agency record. This does not mean, however, that the Department of Justice will disclose all records sought. As noted above, there are statutory exemptions that authorize the withholding of information of a sensitive nature. When the Justice Department does withhold information from you, it ordinarily must specify which exemption of the FOIA permits the withholding. You should be aware that the FOIA does not require agencies to do research for you, to analyze data, to answer written questions, or to create records in order to respond to a request.

Source: Department of Justice. *Freedom of Information Act Reference Guide*. April 2005. http://www.usdoj.gov/04foia/04_1_1.html ; "Subpart A - Procedures for Disclosure of Records Under the Freedom of Information Act." http://www.usdoj.gov/04foia/04_1_1.html, and House Committee on Government Reform. "A Citizen's Guide to the Freedom of Information Act." September 20, 2005, http://www.fas.org/sgp/foia/citizen.html

**FOIA Requester Service Center | FOIA Public Liaisons**

FOIA Requester Service Centers (Center), as appropriate, which shall serve as the first place that a FOIA requester can contact to seek information concerning the status of the person's FOIA request and appropriate information about the agency's FOIA response. The Center shall include appropriate staff to receive and respond to inquiries from FOIA requesters;

Source: Executive Order 13392, "Improving Agency Disclosure of Information," December 14, 2005, http://www.fas.org/irp/offdocs/eo/eo-13392.htm

**Foreground Information**
All information and material jointly generated and funded pertaining to the cooperative program. This information is available for use by all participating governments in accordance with the terms of an MOA [Memorandums of Agreement].

Source: Department of the Army. "Special Access Programs (SAPs) and Sensitive Activities." AR 380-381. April 21, 2004, http://www.fas.org/irp/doddir/army/ar380-381.pdf

**Foreign Broadcast Information Service (FBIS)**
On February 26, 1941, the FCC received funding to launch the "Foreign Broadcast Monitoring Service," the first name for FBIS. Operated by the CIA, FBIS monitors[ed] and translates[d] foreign daily news accounts, commentaries, and government statements from broadcasts, press agency transmissions, newspapers, and periodicals published within the previous 48-72 hours. Separate editions cover East Asia, East Europe, Latin America, Near East and South Asia, Africa (Sub-Sahara), China, former Soviet Union and West Europe.

Found in microfiche in most libraries with a government publications section, and through subscription through World News Connection, which includes full text and summaries of foreign newspaper articles, conference proceedings, television and radio broadcasts, periodicals, and non-classified technical reports. The material in WNC is provided to the National Technical Information Service (NTIS) by the Open Source Center (OSC).

Source. Stephen C. Mercado. "FBIS Against the Axis, 1941-1945." https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v45i5a04p.htm; World News Connection http://wnc.fedworld.gov/ and FAS, Intelligence Resource Program. http://www.fas.org/irp/fbis/

**Foreign Civil Intelligence**
Intelligence derived from all sources regarding the social, political and economic aspects of governments & civil populations, their demographics, structures, capabilities, organizations, people, and events. (This definition has been based on consideration of several alternatives to describe civilian social, political, and economic information: 1) Civil Considerations—the political, social, economic, and cultural factors of and AOR (area of responsibility; Army FM 3-07 paragraph 2.7), 2) Civil Considerations- the influence of manmade infrastructure, civilian institutions, and attitudes & activities of the civilian leaders, populations, and organizations within an AOR on the conduct of military operations (Army FM-06), and 3) "Cultural Intelligence" defined in USMC Urban GIRH; and often cited by Retired General Anthony Zinni).

Source: Defense Advanced Research Project Agency (DARPA). "Urban Sunrise." February 2004, http://www.fas.org/man/eprint/urban.pdf, and Department of the Army Field Manual 3-07 (at globalsecurity.org), http://www.globalsecurity.org/military/library/policy/army/fm/3-07/

**Foreign Government Information (FGI)**

***See Classification***

Defined in Executive Order 12958 (Clinton April 1995):
(1) information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;(2) information produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the are to be held in confidence; or (3) information received and treated as "Foreign Government Information" under the terms of a predecessor order."

Bush Executive Order 13292 makes FGI classified information.

Source: FAS. "White House Conference Call Briefing." http://www.fas.org/sgp/news/2003/03/wh032503.html and National Classification Management Society. *Bulletin*. January-February 2005. 7-8, [See the Wayback Machine, http://web.archive.org/web/20061016081303/http://www.classmgmt.com/newsltr/janfeb05.pdf ]

**Foreign Intelligence Information**

***See Electronic Surveillance***

1. Foreign Intelligence. Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons.

Source: National Security Act of 1947, as amended (50 U.S.C. Chapter 15, 401(a) http://www.gpoaccess.gov/U.S.C.ode/search.html and Executive Order 12333, 3.4. "United States Intelligence Activities." http://www.archives.gov/federal-register/executive-orders/1981-reagan.html

**Foreign Intelligence Surveillance Act (FISA)**

1. The Foreign Intelligence Surveillance Act 50 U.S.C. § 1801 et seq., (FISA) as passed in 1978, provided a statutory framework for the use of electronic surveillance in the context of foreign intelligence gathering. In so doing, the Congress sought to strike a delicate balance between national security interests and personal privacy rights. Subsequent legislation expanded federal laws dealing with foreign intelligence gathering to address physical searches, pen registers and trap and trace devices, and access to certain business records.

Section 218 of the Patriot Act amends the Foreign Intelligence Surveillance Act of 1978, allowing the sharing of foreign intelligence information between agencies, and Section 504, amends the Foreign Intelligence Surveillance Act of 1978 (FISA; 50 U.S.C. 1806), and gives license to intelligence officers to who conduct electronic surveillance to "coordinate efforts" with law enforcement to coordinate investigations.

Source: Elizabeth B. Bazan. "The Foreign Intelligence Surveillance Act. An Overview of the Statutory Framework and Recent Judicial Decisions." *CRS Report to Congress,* Updated September 22, 2004, http://www.fas.org/irp/crs/RL30465.pdf; The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2000, http://purl.access.gpo.gov/GPO/LPS17579, CRS, "Amendments to the Foreign Intelligence Surveillance Act," [n.d.] http://www.fas.org/sgp/crs/intel/m071906.pdf, and *Hepting v.AT&T @* EFF, http://www.eff.org/cases/hepting

2. FISA was based on a simple and important rule. If the surveillance fit within FISA—you either had a warrant or a very specific certification from the Attorney General—then the law was you had to cooperate, whether you were a landlord, whether you were a phone company. You had an obligation to cooperate and you were fully protected from criminal or civil liability if you failed to cooperate. On the other hand, if you cooperated without the warrant or the certification required by the statute, then you were subject to civil and criminal penalties from the State as well as from the Federal Government.

Source: Testimony Morton Halperin (p.67), United States. Congress. House. Committee on the Judiciary. *Warrantless surveillance and the Foreign Intelligence Surveillance Act: the Role of Checks and Balances in Protecting American's Privacy Rights.* Pt. I : Hearing before the Committee on the Judiciary, House of Representatives, One Hundred Tenth Congress, first session, September 5, 2007, Washington : U.S. G.P.O. 2008, http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=110_house_hearings&docid=f:37599.pdf

**Note**: FISA Sections will sunset in December 2009: Section 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA), also known as the "lone wolf" provision; Section 206 of the USA PATRIOT ACT amended FISA to permit multipoint, or "roving," wiretaps by adding flexibility to the degree of specificity with which the location or facility subject to electronic surveillance under FISA must be identified, and Section 215 of the USA PATRIOT ACT enlarged the scope of documents that could be sought under FISA, and lowered the standard required before a court order could be issued compelling the production of documents. See Edward C. Liu "Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009," *CRS Report to Congress* January 6, 2009 R40138, http://www.fas.org/sgp/crs/intel/R40138.pdf

**Foreign Relations of the United States**
***See Advisory Committee on Historical Diplomatic Documentation***

1. The official diplomatic history of the United States.

2. Speaking of the State Department and the timely issuance of FRUS, the Advisory Committee on Historical Diplomatic Documentation stated:
Last year the committee reported that "it is reasonable" to be optimistic that the series would be in compliance with the law by the end of 2010. We no longer have any reason to be optimistic, and are frankly very pessimistic. It seems clear that unless there is a dramatic improvement in the publication schedule, the Department of State will remain significantly out of compliance with the law well into the second decade of the 21st century.

Source: Department of State. 10 FAM 141.2-2, "Foreign Relations of the United States." http://foia.state.gov/REGS/fams.asp?level=2&id=11&fam=0 and Report of the Advisory Committee on Historical Diplomatic Documentation, January 1- December 31, 2007 (issued May 19, 2008), http://fas.org/sgp/advisory/state/hac2007.pdf; also see Office of the Inspector General, *Management Review of the Office of the Historian Bureau of Public Affairs, U.S. Department of State,* May 2009, http://oig.state.gov/documents/organization/124568.pdf

3. (1) We find that the current working atmosphere in the HO and between the HO [sic Historians Office, State] and the HAC [sic Historical Advisory Committee] poses real threats to the high scholarly quality of the FRUS series and the benefits it brings. Remarkably, in all our interviews and the statements we received, only a single person suggested that there was no crisis, no problem beyond what is normal in an office.

(5) We recommend that there be a careful and supportive study of information security issues in the HO that is designed to generate practical solutions to the information security workplace challenges that so many of our interviewees have described.

Source: Warren Kimball, *Report to the Secretary of State of the Review Panel Examining the Impact on the Foreign Relations Series of Current Disputes Related to the Historical Office*, January 18, 2009, FAS http://www.fas.org/sgp/advisory/state/ho-review.pdf; also see Office of the Inspector General, *Management Review of the Office of the Historian Bureau of Public Affairs*, U.S. Department of State, Report Number ISP-I-09-43, May 2009,http://oig.state.gov/documents/organization/124568.pdf

**Foreign Schools Initiatives National Student Loan Data System**
***See Data Mining***
Department of Education. Loan Data System/Central Processing. Is a proactive investigation effort that looks at whether financial aid was granted individuals attending foreign institutions during periods of nonenrollment;
Purpose: Detecting criminal activities or patterns;

Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

### Foreign Terrorist Tracking Task Force Activity

*See Data Mining*

Federal Bureau of Investigation. Supports the Foreign Terrorist Tracking Task Force that seeks to prevent foreign terrorists from gaining access to the United States. Data from the Department of Homeland Security, Federal Bureau of Investigation, and public data sources are put into a data mart and mined to determine unlawful entry and to support deportations and prosecutions;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: Yes;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html and William J. Krouse. "Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6." *CRS Report to Congress* April 21, 2004, http://www.fas.org/irp/crs/RL32366.pdf

### Foreseeable Harm Standard

After taking all of these openness principles into account, there still will be records and portions of records for which protection will remain entirely appropriate. As the Attorney General recognized in his Guidelines, "the disclosure obligation under the FOIA is not absolute." Congress included exemptions from mandatory disclosure to protect against different harms, such as, for example, harm to national security, harm to personal privacy, and harm to law enforcement interests.

Under the Attorney General's Guidelines, before withholding a record, the agency must reasonably foresee that disclosure would harm an interest protected by one of the exemptions. Thus, FOIA professionals should examine individual records with an eye toward determining whether there is foreseeable harm from release of that particular record, or portion thereof. Each record should be reviewed by agencies for its content, and the actual impact of disclosure

for that particular record, rather than simply looking at the type of document or the type of file the record is located in.

Source: Attorney General Holder's FOIA Guidelines Creating a 'New Era of Open Government,' " April17, 2009, http://www.usdoj.gov/oip/foiapost/2009foiapost8.htm

**Formal Access Approval**

Process for authorizing access to classified or sensitive information with specified access requirements, such as Sensitive Compartmented Information (SCI), or Privacy Data, based on the specified access requirements and a determination of the individual's security eligibility and need-to-know.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Formerly Restricted Data (FRD)**

***See National Security Information, Restricted Data***

1. Classified information jointly determined by the DOE and the Department of Defense related to the military utilization of atomic weapons, and removed from the RD category pursuant to section 142d of the Atomic Energy Act, and be adequately safeguarded by as National Security Information (NSI).

Source: Section 142d of the Atomic Energy Act, Los Alamos National Lab. "Definitions." http://www.hr.lanl.gov/SCourses/All/PortionMarking/define.htm, DOE. *Understanding Classification*. Washington, D.C.: U.S. Dept. of Energy, Assistant Secretary for Defense Programs, Office of Classification, 1987, and 10 CFR 1016 §1016.3 "Definitions." http://www.gpoaccess.gov/CFR/index.html[34]

2. FRD are sometimes referred to as "classified atomic energy information." FRD is Born Classified.

Source: Arvin S. Quist. "Security Classification of Information." Chapter 3, http://www.fas.org/sgp/library/quist2/chap_3.html

3. Little difference exists between National Security Information and Formerly Restricted Data except for the cumbersome requirement for joint DoD-DOE determinations on

[34] Quist writes that certain types of secret information related to nuclear materials and processes have their origin in the *MED Security Manual,* (U.S. Engineer Office, Manhattan Engineer District, Nov. 26, 1945,http://www.fas.org/sgp/library/quist2/chap_7.html#15)

declassification and the process for sharing the information with other nations—a process largely redundant with other mechanisms for achieving similar objectives.

Source: Albert Narath. *Report of the Fundamental Classification Policy Review Group.* Chapter 3, http://www.fas.org/sgp/library/repfcprg.html#I43

4. Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

5. Only DOE, NRC, DoD, and NASA can grant access to RD and FRD. Contractors of all other federal agencies must be processed for PCLs (personnel clearance) by the DOE. The minimum investigative requirements and standards for access to RD and FRD are set forth in the *National Industrial Security Program Operating Manual* (NISPOM), Chapter 9.

Source: DoD. *National Industrial Security Program Operating Manual* (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

6. E.O. 12958, amended, does not apply to RD or FRD.

Source: Information Security Oversight Office. Marking Classified National Security Information Booklet. ISOO Implementing Directive No. 1 Effective September 22, 2003, http://www.archives.gov/isoo/training/marking-booklet.pdf

**For Official Use Only (FOUO)**

***See Classification Markings / Control Markings, Unclassified Information***

1. Unclassified information may only be shared with individuals who are determined to have a "need to know" it. Furthermore, DHS employees and contractors must sign a special Non-Disclosure Agreement before receiving access to unclassified FOUO information.

The FOUO label is used within the DHS "…to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy and welfare, the conduct of a federal program, or other programs or operations essential to the national interest."

The following types of information will be treated as FOUO information. Where information cited below also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation as Sensitive Security Information (SSI), then SSI guidance for marking, handling, and safeguarding will take precedence.

(a) Information of the type that may be exempts from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments. Designation of information as FOUO does not imply that the information is already exempt from disclosure under FOIA. Requests under FOIA, for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request.

(b) Information exempt from disclosure per 5 U.S.C. 552a, Privacy Act.
(c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements.
(d) Other international and domestic information protected by statute, treaty, regulation or other agreements.
(e) Information that could be sold for profit.
(f) Information that could result in physical risk to personnel.
(g) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 12958, as amended, will be classified as appropriate.
(h) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.
(i) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.
(j) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.
(k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

Source: Department of Homeland Security Management Directive 11042 "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," May 11, 2004, http://www.fas.org/sgp/othergov/dhs-sbu.html

2. FOUO is not classified information, but information that should be distributed only to persons who need to know the information to be aware of conditions that will help keep the homeland, and hence, the community secure. Within DHS, the caveat "For Official Use Only" will be used to identify SBU information within the DHS community that is not otherwise governed by state or regulation. At this point the designation applies only to DHS advisories and bulletins.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404

3. For Official Use Only (FOUO) is a document designation, not a classification. This designation is used by Department of Defense and a number of other federal agencies to identify information or material which, although unclassified, may not be appropriate for public release.

Source: DoD. Defense Personnel Security Research Center. "Employees Guide to Security Responsibilities," http://www.hq.nasa.gov/office/ospp/securityguide/Home.htm

4. A designation that is applied to *unclassified* information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). The FOIA specifies nine exemptions which may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. They are:

(1) Information which is currently and properly classified.
(2) Information that pertains solely to the internal rules and practices of the agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)
(3) Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
(4) Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like

information in the future, or protect the government's interest in compliance with program effectiveness.
(5) Inter-agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.
(6) Information the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
(7) Records or information compiled for law enforcement purposes that (a) could reasonably be expected to interfere with law enforcement proceedings; (b) would deprive a person of a right to a fair trial or impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others, (d) disclose the identity of a confidential source, (e) disclose investigative techniques and procedures, or (f) could reasonably be expected to endanger the life or physical safety of any individual.
(8) Certain records of agencies responsible for supervision of financial institutions.
(9) Geological and geophysical information concerning wells. b. Information that is currently and properly classified can be withheld from mandatory release under the first exemption category. "For Official Use Only" is applied to information that is exempt under one of the *other* eight categories. So, by definition, information must be unclassified in order to be designated FOUO. If an item of information is declassified, it can be designated FOUO if it qualifies under one of those other categories. This means that (1) information cannot be classified and FOUO at the same time, and (2) information that is declassified may be designated FOUO, but only if it fits into one of the last eight exemption categories (categories 2 through 9).

Source: DoD. DOD 5200.1-R Information Security Program. Appendix C, http://fas.org/irp/doddir/dod/5200-1r/appendix_c.htm

5. "The 'FOUO' markings are no longer operative," an Army spokesman said.

Source: "Human Intelligence Collector Operations," Field Manual FM 2-22.3, September 2006, http://www.fas.org/irp/doddir/army/fm2-22-3.pdf (FOUO marking is still being used in 2009 BTW).

**Note:** Except they are; see Gen. Clapper's policy directive April 7, 2009, "Clarification of Current DoD Policy on Controlled Unclassified Information (CUI)," http://www.fas.org/sgp/cui/ousd040709.pdf

### Forward Tell

The transfer of information to a higher level of command.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Freedom of Information Act (FOIA)**

***See Freedom of Information Exemptions, FOIA Request, Presidential Restrictions***

1. In 1953 Congressmen John Moss, considered the father of the Freedom of Information Act, requested information from the Eisenhower Civil Service Commission to verify its claim that 2,800 federal employees had been fired due to "security reasons." Moss required the information to discern whether these terminations entailed allegations of disloyalty, espionage or other conditions (Moynihan 173). The Civil Service Commission refused to supply the information to Moss, who learned that as a member of Congress, he had no legal recourse to force the Commission to disclose the information. In response, Moss convened the Special Government Information Subcommittee in 1955, "tasked with monitoring executive secrecy" (Moynihan 173). Moss and his committee determined "the right to know has suffered" (Moynihan 173). The Committee's investigations led to greater understanding of security classification in the Executive Branch, how secrecy impairs not only the political participation of Congress, but also damages citizen participation. It would be a long, tortuous eleven years before FOIA was realized (Moynihan 173).

In seeking a model for FOIA, Moss looked for guidance on information rights from the U.S. Constitution, English common law, statutory law and federal case law (Kostyu 462). Moss also incorporated the work of Kent Cooper, Harold Cross and the Freedom of Information Committee, American Society of Newspaper Editors (ASNE) into his draft freedom of information bill. Moss and his subcommittee reached the general conclusion that a model freedom of information legislation should read "all records should be open except as otherwise provided by law."

Source: United States Congress. Senate Committee on Governmental Affairs. *Report of the Commission on Protecting and Reducing Government Secrecy: Hearing before the Committee on Governmental Affairs* (United States Senate, One Hundred Fifth Congress, First Session, May 7, 1997. Washington: Government Printing Office, 1997, http://www.access.gpo.gov/congress/commissions/secrecy/); Paul E. Kostyu. "Nothing More, Nothing Less: Case Law Leading to the Freedom of Information Act." *American Journalism* 12 no. 4 (1995): 464-476; Herbert N. Foerstel. *Freedom of Information and the Right to Know: the Origins and Applications of the Freedom of Information Act.* Westport, CT: Greenwood Press, 1999, and the John Moss Foundation website http://www.johnemossfoundation.org/.

2. FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Each state has its own public access laws that should be consulted for access to state and local records. Each federal agency is responsible for meeting its FOIA responsibilities for its own records.

Source: Department of Justice. "Freedom of Information Act (FOIA)," http://www.usdoj.gov/oip/index.html

3. The Freedom of Information Act (FOIA) establishes a presumption that records in the possession of agencies and departments of the executive branch of the U.S. Government are accessible to the people. This was not always the approach to Federal information disclosure policy. Before enactment of the FOIA in 1966, the burden was on the individual to establish a right to examine these government records. There were no statutory guidelines or procedures to help a person seeking information. There were no judicial remedies for those denied access.

With the passage of the FOIA, the burden of proof shifted from the individual to the government. Those seeking information are no longer required to show a need for information. Instead, the "need to know" standard has been replaced by a "right to know" doctrine. The government now has to justify the need for secrecy.

The FOIA sets standards for determining which records must be disclosed and which records may be withheld. The law also provides administrative and judicial remedies for those denied access to records. Above all, the statute requires Federal agencies to provide the fullest possible disclosure of information to the public. The history of the act reflects that it is a disclosure law.

Source: House Committee on Government Reform. "A Citizen's Guide to the Freedom of Information Act." September 20, 2005, http://www.fas.org/sgp/foia/citizen.html

4. The Freedom of Information Act is an information disclosure statute which, through its exemption structure, strikes a balance between information disclosure and nondisclosure, with an emphasis on the "fullest responsible disclosure." Inasmuch as the FOIA's exemptions are discretionary, not mandatory, agencies may make "discretionary disclosures" of exempt information, as a matter of their administrative discretion, where they are not otherwise prohibited from doing so.

Source: Department of Justice. "Discretionary Disclosure and Waiver." *Freedom of Information Guide*, http://www.usdoj.gov/oip/discretionary.htm; also see: Senator Patrick Leahy on the 42nd Anniversary of the Freedom of Information Act, *Congressional Record* June 25, 2008, http://www.gpoaccess.gov/crecord/index.html

### Freedom of Information Act Exemptions

1. The Freedom of Information Act outlines information that is exempt from disclosure:
Exemption 1 Documents classified for national security reasons

Exemption 2 Internal personnel rules and practices

Exemption 3 Documents exempted by statute

Exemption 4 Trade secrets[35]

Exemption 5 Inter/interagency materials (executive privilege)

Exemption 6 Personnel and medical records

Exemption 7- 7(F) Records "compiled for law enforcement purposes"
Exemption 8 Information used in regulating financial institutions (bank examination reports)

Exemption 9 Geological information about oil wells and water resources

Records Exclusions

Source: Department of Justice. *Freedom of Information Guide*, http://www.usdoj.gov/oip/foi-act.htm ; House Committee on Government Reform. "A Citizen's Guide to the Freedom of Information Act." September 20, 2005, http://www.fas.org/sgp/foia/citizen.html and Gina Marie Stevens and Todd B. Tatelman. "Protection of Security-Related Information." *CRS Report for Congress* September 27, 2006, http://www.fas.org/sgp/crs/secrecy/RL33670.pdf

2. The post 9//11 "Critical Infrastructure Information" (CII), which "relates to the production, generation, transportation, transmission, or distribution of energy; could be useful to a person in planning an attack on critical infrastructure," is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552.
Critical infrastructure information as defined in the Patriot Act ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" ) considered is exempt from FOIA, see Exemption 2.

Source: Gina Marie Stevens. "Homeland Security Act of 2002: Critical Infrastructure Information Act." *CRS Report for Congress* February 28, 2003, http://www.fas.org/sgp/crs/RL31762.pdf and *Freedom of Information Guide*, http://www.usdoj.gov/oip/foi-act.htm

3. Moreover, on October 12, 2001, Attorney General John Ashcroft issued a memorandum that supersedes the Department of Justice FOIA policy memorandum that had been in effect since October 1993. The Ashcroft memo "establishes a new "sound legal basis" standard governing the Department of Justice's decisions on whether to defend agency actions

[35] Warren (292) remarks that FOIA "fails to define what 'trade secrecy' means." Jacqueline M. Warren. "Problems Encountered with Confidentiality Bars on Toxic Substances Disclosure Imposed by Federal Environmental Statutes." *New York University Environmental Law Journal* 2 no. 2 (1993): 292-299. http://www1.law.nyu.edu/journals/envtllaw/issues/vol2/index.html

under the FOIA when they are challenged in court. This differs from the "foreseeable harm" standard that was employed under the predecessor memorandum. Under the new standard, agencies should reach the judgment that their use of a FOIA exemption is on sound footing, both factually and legally, whenever they withhold requested information."

Source: DOJ. Office of Information and Privacy. FOIA Post. "New Attorney General FOIA Memorandum Issued." October 2001, http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm

The Ashcroft memo replaces the "sound legal basis" guidance with a standard of "foreseeable harm."

See definitions of **Sensitive Unclassified Information** and **Confidential,** this work. Also the "Card Memorandum" in Reporter's Committee for Freedom of the Press, *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know.* 6th edition, http://www.rcfp.org/homefrontconfidential/foi.html ; also see "President Obama's FOIA Memorandum and Attorney General Holder's FOIA Guidelines Creating a 'New Era of Open Government,' " http://www.usdoj.gov/oip/foiapost/2009foiapost8.htm (#3" Records should not be withheld merely because they fall within an exemption" is noteworthy).

4. S. 1873 creates the "Biomedical Advanced Research and Development Agency" (BARDA) coordinate and oversee activities that support and accelerate qualified countermeasure or qualified pandemic or epidemic product advanced research and development. " Restricts FACA (Federal Advisory Committee Act) access to information and meetings ; exempts "activities, working groups, and advisory boards of the BARDA shall not be subject to disclosure under section 552 of title 5, United States Code, unless the Secretary or Director determines that such disclosure would pass no threat to national security. Such a determination *shall not be subject to judicial review* [112; emphasis added].

Source: S.1873 "To prepare and strengthen the biodefenses of the United States against the deliberate, accidental, and natural outbreaks of illness, and for other purposes." October 17, 2005. Text at GPO Access, http://frwebgate.access.gpo.gov.

**Free Flow of Information**

***See Government Information, Open Information***

Free flow of information as a means in which open government allows the press, interested individuals, and others to see and hear what is going on in government, and take the initiative to publicize, comment upon, and influence governmental activities.

Source: United States. Advisory Commission on Intergovernmental Relations. *Citizen Participation in the American Federal System*. Washington: Advisory Commission on Intergovernmental Relations, 1980. SUDOC: Y 3.Ad 9/8:2 C 49/2

**Fugitive Documents**

Federal agency publications that are not sent to the Government Printing Office for inclusion in the Federal Depository Library Program (FLDP) which supplies libraries with public (not classified or potentially sensitive) information.

Source: Gil Baldwin. "Fugitive Document s- On the Loose or On the Run." http://www.lib.umich.edu/govdocs/adnotes/2003/241003/an2410d.htm

**Full-pipe surveillance**

Utilized by the FBI when an ISP can't isolate the individual or IP address.

Source: Declan McCullagh, "FBI turns to broad new wiretap method." ZDNet News January 30, 2007, http://news.zdnet.com/2100-9595_22-6154457.html and Paul Ohm, "The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property," *Stanford Law Review*/CIS Symposium 2007, http://stlr.stanford.edu/2008/01/the_olmsteadian_seizure_clause.html

**Fuse | Fuselet**

***See Information Dominance, Information Operations, Information Superiority***

1. …Networking software enables commanders to share -- or fuse -- information from an array of air and ground sensors. This will make the tracking of enemy ground troops, friendly troops and artillery and aircraft easier, experts said.

Source: Gene J. Koprowski. "Gigabyte Battlefields." Spacewar.com January 5, 2006, http://www.spacewar.com/news/Gigabyte_Battlefields.html

2. Army IO is conducted within the context of joint IO, including PSYOPS and deception campaigns to ensure the strategic, theater, and tactical efforts are synchronized and collaborative.

In the aggregate, IO technologies will assist in understanding the battlespace. High-speed processors will fuse information from multiple sources while rapid generation of high-fidelity databases will enable the commander to visualize current and future operations. Bandwidth on demand will facilitate common understanding at all echelons and new antenna configurations will allow dissemination of "real time" information on the move. At the same time, low probability of intercept/low probability of detection signature management will protect friendly information while directed and RF energy will disrupt and deny information to the enemy.

Source: Army Vision 2010. "Information Superiority."
http://www.army.mil/2010/information_superiority.htm

3. A common grid, in combination with a distributed and open architecture, gives us the ability later to go back and fuse information that was collected at previous times or to look at correlations of events

Source: Paul G. Kaminski. "21st Century Battlefield Dominance." *Defense Issues* 11 no. 10 (January 16, 1996), http://www.defenselink.mil/speeches/1996/s19960116-kaminski.html

4. The purpose of the Joint Battlespace Infosphere (JBI) Fuselets Concept of Operations (CONOPS) is to propose an envisioned operational capability for the horizontal and vertical integration, manipulation, and production of value-added actionable information. This proposed capability is enabled by an innovative technology known as a fuselet. Fuselets perform information manipulation functions within an information management framework called the Joint Battlespace Infosphere (JBI).

Source: James R. Milligan. "Draft: Concept of Operations: Joint Battlespace Infosphere (JBI) Fuselets." AFRL/IFSE, Joint Battlespace Infosphere (JBI), Air Force Research Laboratory Information Directorate. June 23, 2004, http://www.fuselet.org/specifications/FuseletCONOPS-V1.1-23Jun04.doc

**Fusion**
In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity.

Source: Department of Defense Dictionary. *DoD of Military and Associated Terms*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Fusion Centers**
1. A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the National Criminal Intelligence Sharing Plan (NCISP).'

Source: Department of Justice. "National Criminal Intelligence Sharing Plan."
http://it.ojp.gov/topic.jsp?topic_id=209

2. a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

Source: U.S. Department of Justice and the U.S. Department of Homeland Security, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, August 2006, http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

3. State and city fusion centers (using the Homeland Security Data Network) are found at the Department of Homeland Security, Federal Support to Fusion Centers @ the Information Sharing Environment, and the Senate Committee on Homeland Security and Government Affairs, "Focus on Fusion Centers: A Progress Report," April 17, 2008 (.pdf and audio of hearing).

Also see EPIC, "Information Fusion Centers and Privacy," http://epic.org/privacy/fusion/

**Futilitarian Society**
A society that will not attempt to solve the problems it faces and often refuses even to face its problems because it fears freedom. Because it fears freedom, it will not allow the experimentation, change, discovery, and adventure necessary to the solution of its problems.

Source: William J. Newman. *The Futilitarian Society.* New York, G. Braziller, 1961.

---

## ~ G ~

**GAMMA (G)**
Unclassified term used to describe a type of sensitive compartmentalized information (SCI).

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

**Genoa II**
***See Advanced Research Development Agency (ARDA), Disruptive Technology Office***

1. Will focus on developing information technology needed by teams of intelligence analysts and operations and policy personnel in attempting to anticipate and preempt terrorist threats to US interests. Genoa II's goal is to make such teams faster, smarter, and more joint in their day-to-day operations. Genoa II will apply automation to team processes so that more information will be exploited, more hypotheses created and examined, more models built and populated with evidence, and in the larger sense, more crises dealt with simultaneously. Genoa II will develop and deploy: 1) cognitive aids that allow humans and machines to "think together" in real-time about complicated problems; 2) means to overcome the biases and limitations of

the human cognitive system; 3) “cognitive amplifiers” that help teams of people rapidly and fully comprehend complicated and uncertain situations; and, 4) the means to rapidly and seamlessly cut across and complement existing stove-piped hierarchical organizational structures by creating dynamic, adaptable, peer-to-peer collaborative networks.

Source: DARPA. “Genoa II” [See the Wayback Machine, http://web.archive.org/web/20020802015004/http://www.darpa.mil/iao/GenoaII.htm ] and Electronic Frontier Foundation (EFF). “Genoa II.” http://www.eff.org/Privacy/TIA/genoaII.php

2. Genoa II, which focused on building information technologies to help analysts and policy makers anticipate and pre-empt terrorist attacks. Genoa II was renamed Topsail when it moved to ARDA, intelligence sources confirmed. (The name continues the program's nautical nomenclature; "genoa" is a synonym for the headsail of a ship.)

As recently as October 2005, SAIC was awarded a $3.7 million contract under Topsail. According to a government-issued press release announcing the award, "The objective of Topsail is to develop decision-support aids for teams of intelligence analysts and policy personnel to assist in anticipating and pre-empting terrorist threats to U.S. interests." That language repeats almost verbatim the boilerplate descriptions of Genoa II contained in contract documents, Pentagon budget sheets, and speeches by the Genoa II program's former managers.

Source: Shane Harris. “TIA Lives on.” *National Journal* Feb. 23, 2006, http://nationaljournal.com/about/njweekly/stories/2006/0223nj1.htm

### Geospatial Information

Foundation information upon which all other battlespace information is referenced to form the common operational picture.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

### Global Information Environment

1. All Individuals, organizations, or systems, most of which are outside the control of the military or National Command Authorities, that collect, process, and disseminate information to national and international audiences.

Source: U.S. Army Field Manual 100-6, “Information Operations,” 1996, http://www.fas.org/irp/doddir/army/fm100-6/

2. All individuals, organizations or systems that collect, process and distribute information. (AFDD 2-5.3)

Source: U.S. Air Force. Public Affairs Operations. Air Force Doctrine Document 2-5.3, June 24, 2005. [See the Wayback Machine, http://web.archive.org/web/20061007174450/http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5.3/afdd2-5.3.pdf ]

**Global Information Grid Defense Sector (GIG)**

The globally interconnected, end-to- end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel including all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in Section 5142 of the Clinger-Cohen Act of 1996.

Source: DoD. DoD Directive 3020.40. Defense Critical Infrastructure Program (D.C.IP). August 19, 2005, http://www.fas.org/irp/doddir/dod/d3020_40.pdf

**Global Information Grid (GIG)**

E2.1.1.1. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (b)). The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

Source: DoD Directive 8100.1 "Global Information Grid (GIG) Overarching Policy." September 19, 2002, http://www.dtic.mil/whs/directives/corres/html/810001.htm

**Global Information Infrastructure (GII)**

1. Worldwide interconnections of the information systems of all countries, international and multinational organizations, and international commercial communications.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

2. The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

### Global Justice Information Sharing Initiative (Global)

The Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee (FAC) and advises the U.S. Attorney General on justice information sharing and integration initiatives. Global was created to support the broad scale exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment.

Global is a "group of groups," representing more than thirty independent organizations spanning the spectrum of law enforcement, judicial, correctional, and related bodies. Member organizations participate in Global with a shared responsibility and shared belief that, together, they can bring about positive change by making recommendations and supporting the initiatives of the U.S. Department of Justice (DOJ).

Source: Department of Justice. Office of Justice Programs. Bureau of Justice Assistance, http://it.ojp.gov/topic.jsp?topic_id=8

### Global Justice XML Data Model

***See Terrorist Watchlist Person Data Exchange Standard, XML***

The Global Justice XML Data Model (Global JXDM) is intended to be a data reference model for the exchange of information within the justice and public safety communities. The Global JXDM is sponsored by the U.S. Department of Justice (DoJ) Office of Justice Programs (OJP), with

development supported by the Global Justice Information Sharing Initiative's (Global) XML Structure Task Force (GXSTF). The following are key links to Global JXDM resources.

Source: Department of Justice. Office of Justice Programs. Information Technology Initiatives, http://www.it.ojp.gov/jxdm/ and http://it.ojp.gov/jxdd/JusticeXMLDataSheet.pdf

### Globalization

The integration of the political, economic and cultural activities of geographically and/or nationally separated peoples – is not a discernible event or challenge. is not new, but it is accelerating. Mostly, globalization is largely irresistible. Thus, globalization is not a policy option, but a fact to which policymakers must adapt.

Globalization has accelerated as a result of many positive factors, the most notable of which include: the collapse of communism and the end of the Cold War; the spread of capitalism and free trade; more rapid and global capital flows and more liberal financial markets; the liberalization of communications; international academic and scientific collaboration; and faster and more efficient forms of transportation. At the core of accelerated global integration – at once its principal cause *and* consequence – is the information revolution, which is knocking down once-formidable barriers of physical distance, blurring national boundaries and creating cross-border communities of all types.

Source: Donald A. Hicks. Office of the Under Secretary of Defense for Acquisition and Technology. *Final Report of the Defense Science Board Task Force on Globalization and Security.* December 1999, http://www.acq.osd.mil/dsb/reports/globalization.pdf

### Glomar Response

***See Freedom of Information Act Exemptions***

1. Such records requesters who seek records concerning specific actual or alleged CIA employees, operations, or sources and methods used in operations will necessarily be informed that we can neither confirm nor deny the existence of any responsive records. This policy is required to protect the confidentiality of such matters where public disclosure of the existence or non-existence of records would lead to the loss or the diminution in value of our intelligence program supporting the nation's leadership.

Source: Central Intelligence Agency. "The Freedom of Information Act 5 U.S.C. §552." http://www.foia.cia.gov/foia.asp

2. A "Glomar" response is an agency's express refusal even to confirm or deny the existence of any records responsive to a FOIA request. This type of response was first judicially recognized in the national security context. *Phillippi v. CIA*, 546 F.2d 1009, 1013 (D.C. Cir.

1976) (raising issue of whether CIA could refuse to confirm or deny its ties to Howard Hughes' submarine retrieval ship, the Glomar Explorer). Although the "Glomarization" principle originated in a FOIA exemption (1) case, it can be applied in cases involving other FOIA exemptions as well, in particular privacy exemptions (6) and (7) (C). A "Glomar" response can be justified only when the confirmation or denial of the existence of responsive records would, in and of itself, reveal exempt information.

Because bureaus and offices occasionally question when it is appropriate to give a "Glomar" response, I am attaching for your information copies of the Department of Justice's (DOJ) guidance on privacy "Glomarization". This information should be helpful in providing advice to your client bureaus and offices on this issue. By copy of this memorandum, I am requesting that the Departmental FOIA Officer forward DOJ's guidance to the bureau and office FOIA Officers. The FOIA Officers should be advised to consult with their designated FOIA attorneys in determining whether to issue a "Glomar" response to a FOIA request.

Source: Department of Justice. September 4, 1998, http://www.doi.gov/foia/glomar.htm

3. Since the early 1980s, the CIA has taken advantage of the "Glomar response," a refusal to confirm or deny the existence of records requested under FOIA. Federal courts almost always accept the Glomar response, and the CIA exploits it so often that the Ninth Circuit (*Hunt v. Central Intelligence Agency*, 981 F.2d 1116, 1120 9th Cir. 1992, noting that "we are now only a short step [from] exempting all CIA records from FOIA") noted it has become "a near-blanket FOIA exemption." Note 150 states that Glomar response arises from a CIA policy first articulated in response to FOIA requests concerning the Glomar Explorer, "a secret underwater vessel."

Source: Ava Barbour. "Ready…Aim…FOIA! A Survey of the Freedom of Information Act in the Post-9/11 United States." *The Boston Public Interest Law Journal* Spring 2004, 13 B.U. *Pub. Int. L.J.* 203.

4. The CIA claimed that any records that might exist which may reveal any CIA connection with or interest in the activities of the Glomar Explorer, or any evidence that might reveal the existence of records of this type would be classified, and therefore, exempt from disclosure under exemption 1 of the FOIA. They also insisted that exemption 3 applied, as the National Security Act of 1947 precluded them from releasing information related to the functions of CIA personnel. This was the first instance of an agency using the "can neither confirm nor deny" answer in response to a FOIA request. Since then, the terms "Glomar response," and "Glomarization" are used to describe an agency's response when they can neither confirm nor deny whether records exist.

Source: FAS. Project Jennifer Hughes *Glomar* Explorer. http://www.fas.org/irp/program/collect/jennifer.htm; Roy Varner, and Wayne Collier. *A Matter of Risk: the Incredible Inside Story of the CIA's Hughes Glomar Explorer Mission to Raise a Russian Submarine* (New York: Random House, 1978), and United States. Congress. Senate. Subcommittee on Administrative Practice and Procedure, *Freedom of Information Act :Hearings before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary*, (United States Senate, Ninety-fifth Congress, first session, on oversight of the Freedom of information act, September 15, 16, October 6, and November 10, 1977. Washington, D.C.: Subcommittee on Administration Practice and Procedure: U.S. GPO, 1978. SUDOC: Y 4.J 89/2: In 3/13), contains detailed exhibits and testimony from the CIA and NSC relating to the *Glomar* incident and the agencies' refusal to release information.

## Google Earth | Google Maps

***See National Security Information***

1. But for all of the places that Google Maps allows you to see, there are plenty of places that are off-limits. Whether it's due to government restrictions, personal-privacy lawsuits or mistakes, Google Maps has slapped a "Prohibited" sign on the following 51 places (The White House, PAVE PAWS, U.S. Air Force …)

Source: IT Security Editors, "Blurred Out: 51Things You Aren't Allowed to See on Google Maps," IT Security, July 15, 2008, http://www.itsecurity.com/features/51-things-not-on-google-maps-071508/

2. Two years have passed since Google startled the world with its free, online, high-resolution mapping products of the world. Foreign governments expressed their shock and concern about such detailed imagery in the hands of the general populace; their facilities and state secrets exposed to the world. "Today, with the advent of civilian satellites here and abroad, we have opened wide the window on places and events that, not so long ago, only spies could see," writes Sharon Weinberger.1 As the initial shock wore off, five main responses to the "Google threat" emerged from nations around the world: negotiations with Google, banning Google products, developing a similar product, taking evasive measures, and nonchalance. This report discusses foreign reporting and government response to the online mapping revolution after the initial brouhaha.

Source: DNI, Open Source Center, "The Google Controversy -- Two Years Later," July 30, 2008, http://www.fas.org/irp/dni/osc/google.pdf

## Gospel of National Security

***See National Security, National Security Information, National Security State***

One can hypothesize that there is a desire among Americans, when it comes to foreign policy, to find a single concept, a Commanding Idea, that explains how America relates to the rest of

the world, that integrates contradictory information, that suggests and rationalizes courses of action, and that, as a court of last resort for both policymakers and public, almost magically puts an end to disputes and debates, If such is the case, then "national security" has been a Commanding Idea for more than three decades of American history (p.196).

And what characterizes the concept of national security? It postulates the interrelatedness of so many different political, economic, and military factors that developments seen to have automatic and direct impact on America's core interests, Virtually every development in the world is perceived to be potentially crucial. An adverse turn of events anywhere endangers the United States. Problems in foreign relations are viewed as urgent and immediate threats. Thus, desirable foreign policy goals are translated into issues of national survival, and the range of threats becomes limitless. (p. 196)

The doctrine is characterized by expansiveness, a tendency to push the subjective boundaries of security outward to more and more areas, to encompass more and more geography and more and more problems. It demands that the country assume of posture of military preparedness; the nation must be on permanent alert. There was a new emphasis on technology and armed force. Consequent institutional changes occurred, All of this leads to a paradox: the growth of American power did not lead to a greater sense of assuredness, but rather to an enlargement of the range perceived threats that must urgently be confronted (p.196)

Indeed the doctrine of national security was a fundamental revision of America's perceived relation to the rest of the world, of what Stimson in 1941 had called "our basic theory of defense." The nation was to be permanently prepared. America's interests and responsibilities were unrestricted and global. National security became a guiding rule, the Commanding Idea. It lay at the heart of a new and sometimes intoxicating vision. (p. 220-221)

Source: Daniel H. Yergin. "The gospel of national security: preparing for war just over the horizon," Shattered *Peace:The Origins of the Cold War and the National Security State*, New York: Penguin Books, 1977.

### Government Information

Information that is owned by, produced by or for, or is under the control of the U.S. Government.

Source: Energy. 10 CFR 1045, http://www.gpoaccess.gov/CFR/index.html

### Government Off the Shelf (GOTS)

IT products that are developed by U.S. government organizations with U.S. Government-related requirements in mind and are designated as available only to other U.S. Government organizations In the context of NSTISSP No. 11 [National Information Assurance Acquisition Policy]; GOTS are Information Assurance or Information Assurance-Enabled products that often require special features and assurances that are not found in typical Commercial-Off-the-Shelf (COTS) products.

Source: U.S Department of State. *Foreign Affairs Manual*. 5 FAM 910,. "Information Technology Acquisition Policies." June 20, 2005, http://www.state.gov/m/a/dir/regs/

**Gray Literature**

***See Grey Literature***

Material not well covered by conventional book trade channels. Information contained within this category is often not available in any other kind of source. Gray literature is intrinsically more difficult to identify, acquire, process, access, and otherwise handle than conventional literature. Examples include, but are not limited to, conference papers, trade literature, electronic bulletin boards, and foreign government reports. The most significant point to make about the value of gray literature is that the information it contains often is not available in any other kind of source.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

**Gray Mail**

***See Classified Information Procedures Act (CIPA), State Secrets Privilege***

The threat by defendants and their counsel to press for the release or disclose sensitive (national security), classified information, or state secrets during a trial.

No defendant shall disclose any information known or believed to be classified in connection with a trial or pretrial proceeding until notice has been given under this subsection and until the United States has been afforded a reasonable opportunity to seek a determination pursuant to the procedure set forth in section 6 of the Classified Information Procedures Act (PL 96-456).

Source: United States. Congress. House. Permanent Select Committee on Intelligence. Subcommittee on Legislation. *Graymail Legislation: Hearings before the Subcommittee on Legislation of the Permanent Select Committee on Intelligence, House of Representatives, Ninety-sixth Congress* (first session, August 7, 1979, September 20, 1979, Washington: U.S. Government Printing Office, 1980. Y 4.In 8/18:G 79) and Louis Fisher. *In the Name of National Security: Unchecked Presidential Power and the Reynolds Case*. Lawrence: University Press of Kansas, 2006, and Larry M. Eig, "The Classified Procedures Information Act:

An Overview," *CRS Report to Congress* 89-172A, March 2,1989, http://www.fas.org/sgp/crs/secrecy/89-172.pdf

### Gray Products

A-6. Products that conceal and/or do not identify a source are known as gray products. Gray products are best used to support operational plans.

Source: DoD. *Psychological Operations,* FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

### Grey Literature

1. Not declassified; downgraded from secret to confidential.

Source: Herbert S. Marks and George F. Trowbridge .*Framework for Atomic Industry; a Commentary on the Atomic Energy Act of 1954.* Washington: BNA Incorporated, 1955.

2. "Information produced on all levels of government, academics, business and industry in electronic and print formats not controlled by commercial publishing i.e. where publishing is not the primary activity of the producing body." (Luxembourg, 1997 - Expanded in New York, 2004).

Source: GreyNet, http://www.greynet.org/

### GSA Sensitive But Unclassified Building Information

Information concerning General Services Administration Public Building Services controlled space including owned, leased or delegated Federal facilities. GSA-SBU-BI includes building designs such as floor plans, construction plans and specifications, renovation/alteration plans, equipment plans and locations, building operating plans, information used for building services contracts and/or contract guard services, or any other information considered a security risk.

Source: Centers for Disease Control. "Manual Guide - Information Security CD.C.-02."
Office of Security and Emergency Preparedness "Sensitive But Unclassified Information." 07/22/2005, http://www.fas.org/sgp/othergov/cD.C.-sbu.pdf.

### Guardian (Program)

***See Suspicious Activity Reports***

Is an information technology system maintained at the Secret level that allows TMU to collect suspicious activity reports (SARs) made to the FBI and review the SARs in an organized way to determine which ones warrant additional investigative follow-up. Guardian's primary purpose is

not to manage cases, but to facilitate the reporting, tracking, and management of threats to determine within a short time span (30 days or less) whether a particular matter should be closed or referred for an investigation. Guardian also facilitates the TRU's work in performing its analytical functions because the reports are available for pattern and trend analysis.

Source: DOJ, FBI, "eGuardian Threat Tracking System  Privacy Impact Assessment for the eGuardian Threat Tracking System," http://foia.fbi.gov/eguardian_threat.htm

**Guidance Documents**
Guidance document means an agency statement of general applicability and future effect, other than a regulatory action, that sets forth a policy on a statutory, regulatory, or technical issue or an interpretation of a statutory or regulatory issue.

(h) ''Significant guidance document'' —
(1) Means a guidance document disseminated to regulated entities or the general public that, for purposes of this order, may reasonably be anticipated to: (A) Lead to an annual effect of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal governments or communities; (B) Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; (C) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights or obligations of recipients thereof; or (D) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in this Executive order;…

Source: Executive Order 13422, January 18, 2007, Further Amendment to Executive Order 12866 on Regulatory Planning and Review, http://www.archives.gov/federal-register/executive-orders/2007.html
Amends: Executive Order 12866 , Regulatory Planning and Review was signed September 30, 1993, http://www.archives.gov/federal-register/executive-orders/1993-clinton.html

---

**~ H ~**

**Hacktivism** (U//FOUO)
(A portmanteau of "hacking" and "activism"). The use of cyber technologies to achieve a political end, or technology-enabled political or social activism. Hacktivism might include website defacements, denial-of-service attacks, hacking into the target's network to introduce malicious software (malware), or information theft.

Source: DHS, *Domestic Extremism Lexicon* Reference Aid March 26, 2009, http://www.scribd.com/doc/14884903/Domestic-Extremism-Lexicon-US-Department-of-Homeland-Security-Reference-Aid

**High 2 Information**

Substantial internal matters, the disclosure of which would risk circumvention of a legal requirement; records that "are related solely to the internal personnel rules and practices of an agency."

Source: U.S. Department of Justice. *Freedom of Information Act Guide*, http://www.usdoj.gov/oip/exemption2.htm#high2

**Historical Review Program**

***See Foreign Relations of the United States***

In the 1980's, then Director of Central Intelligence (DCI) William Casey secured the CIA's operational exemption in return for establishing an Historical Review Program (HRP) to open up the CIA's historical record.

To ensure that releases have historical value, officers select subjects with the advice and guidance of the CIA's History Staff, the DCI's Historical Review Panel, and the general public. Under guidelines laid out for the program, historical records are released except in instances where disclosure would damage national security

Source: CIA, "Special Collections," http://www.foia.cia.gov/historical.asp and
Robert Jervis, "The CIA and Declassification: The Role of the Historical Review Panel" *Passport*, April 2009, http://www.shafr.org/newsletter/2009/Passport0409scan.pdf

**Historically Significant Information**

There is no satisfactory means at present of identifying historically significant information within the vast body of information that is being reviewed and declassified. Accordingly, no priority is given to the declassification and release to the public of such information. (p.8)

Issue No. 2: A board consisting of prominent historians, academicians, and former Government officials would be appointed by the Archivist to determine which events or activities of the U.S. Government should be considered historically significant from a national security and foreign policy standpoint, for a particular year.[36] (p.8)

[36] It is remarkable that a select group of individuals determine the historical significance of actions and events.

Issue No. 11: Not infrequently, requests to agencies from individual members of the public actually hamper the agency's ability to make historically significant records available to the public in general. (p.11)

Source: Public Interest Declassification Board, *Improving Declassification: Report to the President,* December 2007, http://www.archives.gov/pidb/recommendations/

### Historically Valuable

Executive Order 12958, "Classified National Security Information" (the Order), called for a renewed commitment by the Executive branch to the concept of declassification tied to specific deadlines, referred to in the Order as automatic declassification. This direction calls for all 25-year-old and older historically valuable permanent records containing classified national security information to be declassified, exempted, excluded, referred to other interested agencies, or appropriately delayed by December 31, 2006, and each year thereafter, for such records prior to their attaining 25-year-old status. As such, it is important to recognize that December 31, 2006, represents not an end unto itself but rather the beginning of integrating automatic declassification into the fabric of the security classification framework.

Source: Information Security Oversight Office. "Report to the President: An Assessment of Declassification in the Executive Branch." September 21, 2005. http://www.archives.gov/isoo/reports/2005-declassification-report.html

### Homeland Security Advisory System

Established in March 2002, the Homeland Security Advisory System was designed to disseminate information regarding the risk of terrorist acts to federal, state, and local government agencies and the public. The Homeland Security Advisory System combines threat information with vulnerability assessments and provides communications to public safety officials and the public.

- **Homeland Security Threat Advisories** contain actionable information about an incident involving, or a threat targeting, critical national networks or infrastructures or key assets. They could, for example, relay newly developed procedures that, when implemented, would significantly improve security or protection. They could also suggest a change in readiness posture, protective actions, or response. This category includes products formerly named alerts, advisories, and sector notifications. Advisories are targeted to Federal, state, and local governments, private sector organizations, and international partners.

- **Homeland Security Information Bulletins** communicate information of interest to the nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of warning messages. Such information may include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. It also may include preliminary requests for information. Bulletins are targeted to Federal, state, and local governments, private sector organizations, and international partners.
- **Color-coded Threat Level System** is used to communicate with public safety officials and the public at-large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood or impact of an attack. Raising the threat condition has economic, physical, and psychological effects on the nation; so, the Homeland Security Advisory System can place specific geographic regions or industry sectors on a higher alert status than other regions or industries, based on specific threat information. Colors are: Green (Low Risk), Blue (Guarded Risk), Yellow (Elevated Risk), Orange (High Risk), and Red (Severe Risk).

Source: Department of Homeland Security. "Citizen Guidance on the Homeland Security Advisory System." http://www.dhs.gov/dhspublic/display?theme=29; http://www.dhs.gov/interweb/assetlibrary/CitizenGuidanceHSAS2.pdf and General Accounting Office (GAO). "Homeland Security Advisory System: Preliminary Observations Regarding Threat Level Increases from Yellow to Orange." March 11, 2004. GAO-04-453R, http://www.gao.gov/htext/d04453r.html

**Homeland Security Information**

***See Sensitive But Unclassified Information***

1. Any information possessed by a Federal, State or local agency that

(A) relates to the threat of terrorist activity;
(B) relates to the ability to prevent, interdict, or disrupt terrorist activity;
(C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or
(D) would improve the response to a terrorist act.
(E)

Source: Library of Congress. "Laws and Regulation Governing the Protection of Sensitive But Unclassified Information." http://www.loc.gov/rr/frd/pdf-files/sbu.pdf ; also see Andrew Card. ("The Card Memo") "Guidance on Homeland Security Information Issued." March 21, 2002, [See the Wayback Machine, http://web.archive.org/web/20080306140939/http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm] and Mark A, Randol, "Homeland Security Intelligence: Perceptions, Statutory Definitions and Counter-Terrorism," CRS Report for Congress January 14, 2009, RL33616,

http://www.fas.org/sgp/crs/intel/RL33616.pdf

2. The 9/11 Commission and others have observed that the over-classification of homeland security information interferes with accurate, actionable, and timely homeland security information sharing, increases the cost of information security, and needlessly limits public access to information. (Section 2: Findings (2))

Source: H.R.553 Reducing Over-Classification Act of 2009, *Congressional Record*, 155 (February 3, 2009), http://www.gpoaccess.gov/crecord/

**Homeland Security Information Bulletins**

***See Homeland Security Advisory System***

Communicate information of interest to the nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of warning messages.

Source: Department of Homeland Security, http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0335.xml

**Homeland Security Information Network (HSIN)**

1. In February 2004, the Department of Homeland Security (DHS) announced the launch of its Homeland Security Information Network (HSIN) initiative, designed to connect all 50 states, five U.S. territories, and 50 major urban areas with the Homeland Security Operations Center (HSOC) at the department. To accomplish this goal, DHS adopted the JRIES infrastructure, expanding both its capabilities and its community of users beyond its original "law enforcement and intelligence counterterrorism mission" while leaving the original JRIES system in place.

Source: Harold C. Relyea and Jeffrey W. Seifert. "Information Sharing for Homeland Security: A Brief Overview." *CRS Report to Congress* January 10, 2005, http://www.fas.org/sgp/crs/RL32597.pdf

2. The Homeland Security Information Network (HSIN) allows all states and major urban areas to collect and disseminate information between federal, state, and local agencies involved in combating terrorism.

- helps provide situational awareness
- facilitates information sharing and collaboration with homeland security partners throughout the federal, state and local levels
- provides advanced analytic capabilities
- enables real time sharing of threat information

This communications capability delivers to states and major urban areas real-time interactive connectivity with the National Operations Center.

Source: DHS, http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm and GAO, *Information Technology: Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives*, GAO-07-822T, May 10, 2007, http://www.gao.gov

**Homeland Security Intelligence (HSINT)**

1. Could likely be defined as a more refined and finished version of homeland security *information*. The nexus to terrorism and terrorist-related events is direct and compelling. One complication of discerning what is homeland security information remains how the investigator or operator knows that the activity which they are investigating or monitoring is related to terrorism…

Source: Todd Masse, "Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches" CRS Report for Congress August 18, 2006, RL33616, http://www.fas.org/sgp/crs/intel/RL33616.pdf

2. There are at least three different constructs that could be used to frame HSINT: (1) geographic structural, and (3) holistic (p.11).

An intelligence approach that considered only activities associated with homegrown threats, without a more integrated, global perspective on the threat, would miss one of the central lessons learned from 9/11—the importance of integrating intelligence related to threats to national security regardless of the geographic location of the source. (p.12)

Source: Mark A, Randol, "Homeland Security Intelligence: Perceptions, Statutory Definitions and Counter-Terrorism," *CRS Report for Congress* January 14, 2009, RL33616, http://www.fas.org/sgp/crs/intel/RL33616.pdf

**Homeland Security Intelligence Community**

Includes the organizations of the Stakeholder community that have intelligence elements.

Source: Department of Homeland Security, *DHS Intelligence Enterprise Strategic Plan*, January 2006, http://www.fas.org/irp/agency/dhs/stratplan.pdf and Mark A, Randol, "Homeland Security Intelligence: Perceptions, Statutory Definitions and Counter-Terrorism," *CRS Report for Congress* January 14, 2009, RL33616, http://www.fas.org/sgp/crs/intel/RL33616.pdf

**Homeland Security Operations Morning Brief**

Comprised of mostly suspicious activity reports minus any information on U.S. persons contained within criminal intelligence protected by privacy laws, is shared on a Sensitive but

Unclassified (SBU) level with about 1500 Federal, State, and local intelligence and law enforcement agencies and subscribers.

Source: Matthew E. Broderick, Director Homeland Security Operations Center. Statement before the House Committee on Homeland Security, Intelligence, Information Sharing, and Terrorism Risk Assessment Subcommittee, July 20, 2005, http://bulk.resource.org/gpo.gov/hearings/110h/27686.pdf

**Homeland Security Threat Advisories**
***See Homeland Security Advisory System***

Actionable information about an incident involving, or a threat targeting, critical national networks or infrastructures or key assets.

Source: Department of Homeland Security,
http://www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm

**Horizontal Fusion**
***See Global Information Grid***

Horizontal Fusion, begun in January 2003, is an award-winning Department of Defense Transformation initiative that brings together a collection of 31 initiatives focused on enabling true net-centric warfare. Horizontal Fusion is at the leading edge of transforming the DOD through a portfolio of initiatives that are breaking down the walls between diverse information stores in the defense, intelligence, diplomatic, and coalition communities and Web-enabling these tools to create a new "Internet for the DOD." Horizontal Fusion is not only helping to establish the standards for security, cross domain information- sharing, tactical wireless, and other tools, it is also putting them into practice. Indeed, current initiatives have already begun to make more information available to those who need it, when they need it.

The Horizontal Fusion Portfolio includes initiatives that will provide the information standards and the Net-Centric Enterprise Services (NCES) required to support net-centric operations. The Global Information Grid (GIG) Bandwidth Expansion (GIG-BE) will increase terrestrial communications capacity, the Joint Tactical Radio System (JTRS) will provide interoperable wireless communications by users of programmable radios, and the Transformational Satellite (TSAT) Communications will make high bandwidth information sources available to DoD "edge users"-warfighters, analysts, commanders, joint forces and coalition partners. Each initiative represents a strategic investment in present and future capabilities that will empower DoD edge users.

Source: DoD. "What is Horizontal Fusion?"

http://horizontalfusion.dtic.mil/faq/ and Gunner Palace [DVD]. Produced, written and directed by Michael Tucker and Petra Epperlein. New York: Palm Pictures, 2005.

**Horizontal Integration**

1. Refers to the desired end-state where intelligence of all kinds flows rapidly and seamlessly to the warfighter, and enables information dominance warfare.

Source: Jason Program Office, Mitre Corporation. "Horizontal Integration: Broader Access Models for Realizing Information Dominance. http://www.fas.org/irp/agency/DoD/jason/classpol.pdf

**Human Environment**

***See Environmental Impact Statement***

Interpreted comprehensively to include the natural and physical environment and the relationship of people with that environment. (See the definition of "effects" (Sec. 1508.8).) This means that economic or social effects are not intended by
themselves to require preparation of an environmental impact statement. When an environmental impact statement is prepared and economic or social and natural or physical environmental effects are interrelated, then the environmental impact statement.

Source: 40 CFR 1508.14. "Definitions." http://www.gpoaccess.gov/cfr/index.html

**Human Terrain System**

1. HTS is a new proof-of-concept program, run by the U.S. Army Training and Doctrine Command (TRADOC), and serving the joint community. The near-term focus of the HTS program is to improve the military's ability to understand the highly complex local socio-cultural environment in the areas where they are deployed;

The HTS approach is to place the expertise and experience of social scientists and regional experts, coupled with reach-back, open-source research, directly in support of deployed units engaging in full-spectrum operations.

Source: U.S. Army Training and Doctrine Command (TRADOC), "Human Terrain System," http://humanterrainsystem.army.mil/, http://humanterrainsystem.army.mil/missionstatement.html, and Hugh Gusterson, "The U.S. military's quest to weaponize culture," Bulletin of the Atomic Scientists June 20, 2008,http://www.thebulletin.org/web-edition/columnists/hugh-gusterson/the-us-militarys-quest-to-weaponize-culture

2. At times, the lexicon we come up with for new programs appears almost designed to induce maximum paranoia. In that vein, "Human Terrain Teams" follows in the proud tradition

of initiatives like: The Office of Special Plans; TALON Reporting System; and Total Information Awareness.

Source: Robert Gates, Address to the Association of American Universities, Washington, D.C., April 14, 2008, http://www.defenselink.mil/speeches/speech.aspx?speechid=1228 and Hugh Gusterson, "The U.S. military's quest to weaponize culture," *Bulletin of the Atomic Scientists* June 20, 2008, http://www.thebulletin.org/web-edition/columnists/hugh-gusterson/the-us-militarys-quest-to-weaponize-culture

**HUMINT Manager**

***See Intelligence Information, National Clandestine Service***

The DCIA will become the National HUMINT manager. He will delegate his day-to-day responsibilities as the National HUMINT manager to the Director of the NCS. The creation of the NCS [National Clandestine Service] will further enhance of the Intelligence Community's (IC) clandestine HUMINT (Human Intelligence) capabilities and create a truly national clandestine HUMINT capability. It will be successful due to the full participation of all relevant IC members.

Source: Central Intelligence Agency Fact Sheet "Creation of the National HUMINT Manager." October 13, 2005, https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/fs10132005.html

---

**~ I ~**

**Icon**

1. Refers to categories of "information that are reflexively classified, without serious evaluation of any national security threat their release might pose. These icons are rarely or never declassified, no matter what the law, or the U.S. Constitution might say."

Source: FAS. *Secrecy News* April 23, 2001. http://www.fas.org/sgp/news/secrecy/2001/04/042301.html

2. All to [*sic* too] often, when government agencies deploy the (b) (1) and (b) (3) [FOIA] exemptions, it has been to ensure continued secrecy for what can be called "classification icons," which are entire categories of information that declassification reviewers reflexively classify without any fresh thinking about the relevance of continued secrecy. Among those "icons" are intelligence spending, the locations of historic nuclear weapons sites, nuclear weapons stockpile information, and the war plans that constitute the SIOP (the Single Integrated Operational Plan for nuclear war).

Source: "Dubious Secrets." National Security Archive Electronic Briefing Book No. 90, Jeffrey Richelson, William Burr and Thomas Blanton (Eds.), 2003,http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB90/index.htm

**Inadequate Record Keeping (Detainees)**

One of the fundamental tenets of the laws of war is that full and adequate records regarding the capture and treatment of detainees must be kept; a host of Department of Defense and Army regulations codify this requirement. Yet in more than a dozen cases, these regulations were not followed, and investigations into most of these detainee deaths appear to have been undermined as a result.

The Army's medical record-keeping was particularly poor, with detainees. medical records often left incomplete or entirely missing. Thus, although Army investigations found that fourteen detainees died of natural causes because of pre-existing conditions, at least five case files do not include records documenting these conditions. In some instances, this appears to have been an administrative oversight by criminal investigators who may not have requested records. In others, however, there were simply no medical records to be found.

Source: Hina Shamsi and Deborah Pearlstein (ed), *Command's Responsibility's Detainee Deaths in U.S. Custody in Iraq and Afghanistan*, Human Rights First, February 2006, http://www.humanrightsfirst.org/us_law/etn/dic/index.asp; also see the Taguba Report with Annexes http://www.dod.mil/pubs/foi/detainees/taguba/

**Inadvertent Disclosure**

1. Type of incident involving accidental exposure of information to an individual not authorized access.

Source: Committee for National Security Systems (CNSS). Instruction 4009.*NationalInformation Assurance Glossary*, June, 2006. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf ; also see DOE, Office of Classification and Information. Twenty-second Report to Congress on Inadvertent Disclosures of Restricted Data under Executive Order 12958, August 2006, http://www.fas.org/sgp/othergov/doe/inadvertent22.pdf

**Incident**

***See Information Operations***

In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. (JP 3-13).

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17, October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Incident Data Mart**

***See Data Mining***

Department of Homeland Security. Will look through incident logs for patterns of events. An incident is an event involving a law enforcement or government agency for which a log was created (e.g., traffic ticket, drug arrest, or firearm possession). The system may look at crimes in a particular geographic location, particular types of arrests, or any type of unusual activity;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Planned;
Features: Personal information: Yes;
Features: Private sector data: Yes;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*.GAO-04-548, May 4, 2004. http://www.gao.gov/htext/d04548.html

**Indications and Warning**

Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/nonnuclear attack on the United States, its overseas forces, or allied and/or coalition nations; hostile reactions to US reconnaissance activities; terrorists' attacks; and other similar events.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Indirect Information Warfare**

Changing the adversary's information by creating phenomena that the adversary must then observe and analyze.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995.
[See the Wayback Machine, http://tinyurl.com/ydvgypl ]

**Influence Operations**

Employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a
change in the adversary decision cycle, which aligns with the commander's objectives. (AFDD 2-5)

Source: U.S. Air Force. Public Affairs Operations. Air Force Doctrine Document 2-5.3, June 24, 2005. [See the Wayback Machine, http://tinyurl.com/ycntjj5 ]

**Info**

***See Procedure Word***

A procedure word meaning, "The addressees immediately following are addressed for information."

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Infoblockade**

*See Information Warfare*

An information warfare attack may also make transport of people and products impossible, paralyzing an economy, and it too may block the spread of information (especially as in an "infoblockade"). (p.19)

Source: Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Information Warfare and International Law,* National Defense University Press, 1998, http://www.dodccrp.org/html4/books_downloads.html

**Informant**

A person who, wittingly or unwittingly, provides information to an agent, a clandestine service, or the police. 2. In reporting, a person who has provided specific information and is cited as a source.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Information**

***See Classification, Free-Flow of Information, Government Information, Open Information***

1. Any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual.

Source: Office of Management and Budget, Circular No. A-130, "Management of Federal Information Resources." February 8, 1996, http://www.whitehouse.gov/omb/circulars/a130/a130.html

2. Information means any statement or estimate of fact or opinion, regardless of form or format, whether in numerical, graphic, or narrative form, and whether oral or maintained on paper, electronic or other media. "Information" does not generally include items in the following categories; however, OMB may determine that any specific item constitutes "information":

(1) Affidavits, oaths, affirmations, certifications, receipts, changes of address, consents, or acknowledgments; provided that they entail no burden other than that necessary to identify the respondent, the date, the respondent's address, and the nature of the instrument (by contrast, a certification would likely involve the collection of "information" if an agency conducted or sponsored it as a substitute for a collection of information to collect evidence of, or to monitor, compliance with regulatory standards, because such a certification would generally entail burden in addition to that necessary to identify the respondent, the date, the respondent's address, and the nature of the instrument); (2) Samples of products or of any other physical objects; (3) Facts or opinions obtained through direct observation by an employee or agent of the sponsoring agency or through nonstandardized oral communication in connection with such direct observations; (4) Facts or opinions submitted in response to general solicitations of comments from the public, published in the Federal Register or other publications, regardless of the form or format thereof, provided that no person is required to supply specific information pertaining to the commenter, other than that necessary for self-identification, as a condition of the agency's full consideration of the comment;(5) Facts or opinions obtained initially or in follow-on requests, from individuals (including individuals in control groups) under treatment or clinical examination in connection with research on or prophylaxis to prevent a clinical disorder, direct treatment of that disorder, or the interpretation of biological analyses of body fluids, tissues, or other specimens, or the identification or classification of such specimens; (6) A request for facts or opinions addressed to a single person; (7) Examinations designed to test the aptitude, abilities, or knowledge of the persons tested and the collection of information for identification or classification in connection with such examinations; (8) Facts or opinions obtained or solicited at or in connection with public hearings or meetings; (9) Facts or opinions obtained or solicited through nonstandardized follow-up questions designed to clarify responses to approved collections of information; and (10) Like items so designated by OMB.

Source. Office of Management and Budget. 5 CFR 1320. "Controlling Paperwork Burdens on the Public." http://www.gpoaccess.gov/cfr/index.html

3. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. March 28, 2003, http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and Executive Order 13292, "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

4. Knowledge that can be communicated by any means.

Source: U.S. Department of Justice. United States Marshals Service. Office of Inspections. Internal Security Division. *Information Security*. Washington D.C.: 1991. SUDOC: J 25.2: In 3

5. An instance of an information type.

Source: Federal Information Processing Standards 199 (FIPS). *Standards for Security Categorization of Federal Information and Information Systems*. February 2004.

6. Data and instructions.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995, [See the Wayback Machine, http://tinyurl.com/ydvgypl ]

7. (DOD) 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of known conventions used in their representation. (NATO) Unprocessed data of every description which may be used in the production of intelligence. (Army) 1. In the general sense, the meaning humans assign to data. 2. In the context of the cognitive hierarchy, data that have been processed to provide further meaning.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Information Assurance (IA)**

1. Measures that protect and defend information and information systems by ensuring their availability. Integrity, authentication, confidentiality, and nonrepudiation. These measures

include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Source: Committee for National Security Systems (CNSS). Instruction 4009. National Information Assurance Glossary, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

2. (DOD) Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. See also information; information operations; information system.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

### Information Attack

Directly corrupting information without visibly changing the physical entity within which it resides.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995, [See the Wayback Machine, http://tinyurl.com/ydvgypl ]

### Information Box

A DoD and NATO term: A space on an annotated overlay, mosaic, map, etc., which is used for identification, reference, and scale information.

Source: Department of Defense. *DoD of Military and Associated Terms. Amended*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

### Information Bureaucratization

*See Secrecy, Secrets*

Information bureaucratization arises from Max Weber's work in governmental and judicial bureaucracy, especially his ideas regarding files and record keeping practices. Modern organizations, as Weber noted, both generate and are dependent, upon written documents, or the files. Information bureaucratization in Weber's thoughts and manifests in the ways information is gathered, secreted, partitioned, territorialized, manufactured, balkanized, restricted, historically engineered, organized, legitimated, and reified within administrative

units of the United States government and other bureaucratic information machines. [37] These "conditions of information," which also include the mission-specific, regulatory, and statutory language regarding information, obstruct debate about participation, risk, informed consent, self-determination.

Source: Definition – Maret, based on *Max Weber on Law in Economy and Society*. Trans. Edward Shils and Max Rheinstein. Max Rheinstein (Ed.). New York: Simon and Schuster, 1968.

### Information Collection Budget (ICB)

Requires that each agency develop and submit annually a comprehensive budget for all collections of information from the public to be conducted or sponsored by the agency in the succeeding 12 months. The ICB is expressed in the number of hours required of the public to comply with request and requirements for information.

The ICB is the vehicle through which OIRA [Office of Information and regulatory Policy], in consultation with each agency, sets "annual agency goals to reduce information collection burdens imposed on the public." In addition, the ICB serves as a management tool. Agency officials can use the ICB in their internal planning and control processes to review all of the collections of information their staff plans to implement during the forthcoming year. OMB uses the ICB in conjunction with management reviews of other agency activities to assess information collection priorities and to help maintain the lowest necessary level of paperwork burden on the public, consistent with the Federal Government's need for information.

The PRA requires that agencies obtain OMB approval for collections of information. A collection of information without current OMB approval constitutes a violation of the PRA. Each year OMB is required to report to Congress PRA violations published in the Information Collection Budget of the United States.[38]

Source: 5 CFR 1320.10 http://www.gpoaccess.gov/cfr/index.html, and OMB, Executive Office of the President. "Reports to Congress Under the Paperwork Reduction Act of 1995," [See the Wayback Machine, http://web.archive.org/web/20080307102929/http://www.whitehouse.gov/omb/inforeg/prarep2.html ]

### Information Crime | Information Criminal

***See Censorship, Graymail, Leak, Nuclear Secrecy, Propaganda, Secret, Secrecy, State Secrets***

---

[37] Balkanized in the sense of a "fragmentary state," arises from the chaos of Eastern Europe after the collapse of the Soviet Union.

[38] According to OIRA's Fiscal Year 2005 *Managing Information Collection: Information Collection Budget of the United States*, "… the public spent about 7.971 billion hours responding to or complying with information requirements. This represents a 1.6% decrease compared to last year's total of 8.099 billion hours." See http://www.whitehouse.gov/OMB/inforeg/2005_icb_final.pdf

**Note**: the following is a definition is a work in progress. No formal definition exists.
The term was first spotted in *Dismantling Utopia: How Information Ended the Soviet Union*. In this work, the 1985 case of Andrei Mironov is reported. Mr. Mironov was prosecuted under the Article 70 of the *Criminal Code*, which prohibited "anti-Soviet agitation and propaganda with the goal of undermining and weakening the Soviet state and social system." Mironov was sentenced to four years incarceration and three years in exile, and sent to the Dubroulog Prison Camp. He was released from prison in 1987 under Gorbachev regime. Mr. Mironov's crime was being a part of a *samizdat* "ring" that obtained, copied, and circulated illegal foreign literature and research.[39]

A more recent example of an information crime is the 2005 incarceration of Chinese journalist Shi Tao, convicted with the assistance of Yahoo!. Shi Tao was arrested, imprisoned, and sentenced for ten years in prison for sending Yahoo! email on the role of the Chinese government in the Tiananmen Square massacre. Chinese authorities accused him of "illegally providing state secrets to foreign entities."

We might theoretically position the aforementioned cases as *information crimes.* No formal definition of information crime exists; the term is implied in state prosecution of espionage, leaks, and disclosure of sensitive or potentially politically explosive information. There are certain characteristics of an information crime suggested by institutional structures of law and regulation that govern control of information, and informally as a political "thought control," censorship, or in instances of imposed cultural change.

Technology [email, encryption, software, computers in general] and certain techniques such as redaction of information or graymail, are involved in some way. An information crime carries with it some type of penalty for disclosure, which may includes harassment, monetary fines, incarceration, silencing, and other means of punishing individuals or groups. Further, an information crime may have a corollary with the motives and penalties behind the *leak*, especially Hess' typology of a "Whistleblower Leak," which is "usually used by career personnel; going to the press may be the last resort of frustrated civil servants who feel they cannot resolve their dispute through administrative channels." Daniel Ellsberg and the Pentagon Papers is one such example.

[39] *Samizdat* has no official definition; it is a Russian abbreviation of state publishing houses *Gospolitizdat* or *Akademizdat.* Literally translated, means self-published, unofficially distributed literary works, which include political writings, newsletters, open letters, trial transcripts; *samizdat* is often likened to materials of a political nature (Loeber 84, 99-101).

The above cases illustrate that individuals are often singled out in order for governments to maintain tight control over information in attempt to maintain dominance over public perception; bracketing the role of individuals or groups in any information "crimes," can we establish that governments and states are responsible for committing "information crimes" through the overclassification of information, restricting information through executive or deliberative privilege, the misapplication of FOIA exemptions, introduction of disinformation, use of video news releases, or stubbornly refusing the release of critical historical information (as in the instances of the CIA and the Foreign Relation of the United States [FRUS] series)? [40]

Closely linked to censorship, manipulation of information [the tampering or alteration of a set of facts, records, databases, or archives], and government, military, patent, and national security secrecy, it is important to note that an information crime is essentially tied to Sissela Bok's (1989:19) idea of secrecy as "power over controlling the flow of information." The following example from the Chapter 13 of the Advisory Committee on Human Radiation Experiments illustrates my point:

> In the case of research related to chemical and biological warfare, the military issued a secret edict that published articles be cleansed of any reference to military purpose. **[70]** In many cases the opportunity to obscure the full purpose of research by careful wording was obvious. As a DOD document put it, "the term 'radiobiology' is so flexible semantically that, depending upon the investigator's point of view, any project could be classified as 'clinical' or 'basic' or 'nuclear weapons effects.' "**[71]**
>
> Footnotes to the above quote: 70. W. G. Lalor, Rear Admiral, U.S. Navy (Ret.), Secretary, Joint Chiefs of Staff, to Chief of Staff, U.S. Army et al., 3 September 1952 ("Security Measures on Chemical Warfare and Biological Warfare") (ACHRE No. NARA-012495-A), 2. In the memo to the service chiefs of staff, the Joint Chiefs decreed that "responsible agencies" should "[e]nsure, insofar as practicable, that all published articles stemming from the BW [biological warfare] or CW [chemical warfare] research and development programs are disassociated from anything which might connect them with U.S. military endeavor." 71. Office of the Director of Defense Research and Engineering, Thirtieth Joint Medical Research Conference, minutes of 8 January 1964 (ACHRE No. DOD-062994-A), 3.

Although the term *information crime* or *information criminal* is not used, historical parallels of

[40] Not just restriction of information in regard to FRUS, but can the passing on of names by the CIA to the Indonesian Army in 1965-1966 also considered an information crime? I think this question is worth pondering in terms of [information] ethics.

such crimes against the public flow of information rest with the sedition acts in England [the information excesses of the Star Chamber, the Licensing Order of 1643; see Milton's *Areopagitica: A Speech for the Liberty of Unlicensed Printing*], and the July 14, 1798 [Alien] Sedition Act in the United States. Certain propaganda crimes of states and government [National Socialist Germany for example; also see Nancy Snow's work on war and propaganda in the U.S.] may also fall into the category of a government information crime.

Examples of information crimes are replete in dystopian literature. For example, the information crimes of *1984's* Winston Smith in keeping a personal diary and *Going Down the Memory Hole* [there are numerous other examples]; Ray Bradbury's *Fahrenheit 451,* with its covertly stashed texts, book burning, and penalties for knowledge dissemination, illustrate the force and potential of information to alter the course of action and consensus reality.

**A working definition of *information crime* is proposed:**

1. Those acts which involve the gathering, revelation, communication, or sharing of politically explosive, sensitive, censored, contrary, or secret information or forbidden knowledge, considered potentially damaging by a government, a state, an organization or an individual, and has the potential for embarrassment or challenging existing ideologies, policies, and political structures, and carries with it prosecution and penalties for disclosure; 2. espionage or disclosure of secret, sensitive, or other information considered strategic to a foreign country, government, state or organization; 3. information crimes are those acts carried out by states or governments that involve secreting, restricting, altering, or censoring information, as well as the destruction and tampering of databases, records, and archives. An information crime may also involved illegal government spying, surveillance, invasion of privacy, covert recordkeeping, and manipulation of public information through the scientific literature mass media or press; 4. potentially illegal and destructive acts such as hacking, tampering, erasing, or destroying technology or data by governments, states, groups, or individuals.[41]

---

[41] The "ethics of hacking" is a controversial subject; however, the issue begs the question that do *all* cases of hacking imply criminal behavior? The classic "The Hacker Manifesto" characterizes hacking as almost a form of "information liberation" : "We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals…You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity…" [See The Mentor's "The Hacker's Manifesto,http://www.technozen.com/manifesto.htm, originally published in the legendary magazine *Phrack*, 7, Pekka Himanen's *The Hacker Ethic, and the Spirit of the Information Age.* [New York : Random House, 2001], and the Department of Homeland Security's definition, this work].

Depending on the act and who is responsible for carrying it out, the entire notion of an "information crime" violates the spirit of numerous human rights declarations and principles [for example, the *International Covenant on Civil and Political Rights*, the *Universal Declaration of Human Rights*, specifically Article 19, the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, and other instruments].

Source: Proposed definition, Maret; Scott Shane, *Dismantling Utopia: How Information Ended the Soviet Unio*n. [Chicago: Ivan R. Dee, 1994]; N. Belinkova, "Unofficial Censorship." [*Studies on the Soviet Union* 11 (1971): 73-92]; D.A. Loeber, "Samizdat under Soviet law." [In D.D. Barry, et al. (Ed.), *Contemporary Soviet Law: Essays in Honor of John N. Hazard.* The Hague: Martinus Nijhoff, 1974]; Reporters Without Borders, "Information supplied by Yahoo! helped journalist Shi Tao get 10 years in prison," http://www.rsf.org/article.php3?id_article=14884; Stephen Hess, *The Government/Press Connection: Press Officers and their Offices*. [Washington, D.C.: Brookings Institution, 1984. 77-79]; and Sissela Bok. *Secrets*. [New York: Vintage Books, 1989]. **Also see** Stephen Kotkin's [1992] "Terror, Rehabilitation, and Historical Memory: An Interview with Dmitrii Iurasov" [*Russian Review 5,* 238-262] on the Memorial Project in the Russian Federation, and Antoon de Baets' *Censorship of Historical Thought: A World Guide 1945-2000* [Greenwood Press, 2002] for a panoramic, cross-cultural view of censorship and information crimes. This latter work pays homage to those people who only crime was the gathering and sharing of information, a process that Bucky Fuller characterized as the "primary human activity."

### Information Differential

Superior access to and the ability to effectively employ information on the strategic, operational and tactical situation which advanced US technologies provide our forces. Space power is crucial, but does not operate alone, in assisting the joint force to enjoy superiority in command, control, communications, intelligence, navigation, and information processing.

Source: Joint Chiefs of Staff. *Joint Doctrine Encyclopedia*. July 16, 1997, http://www.dtic.mil/doctrine/joint_doctrine_encyclopedia.htm

### Information Domain

The information domain is where information lives. It is the domain where information is created, manipulated, and shared. It is the domain that facilitates the communication of information among warfighters. It is the domain where the command and control of modern military forces is communicated, where commander's intent is conveyed.

Source: David S. Alberts, et al, *Understanding Information Age Warfare* , DoD CCRP, August 2001, p. 12, http://www.dodccrp.org/files/Alberts_UIAW.pdf

### Information Dominance

1. The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary.

Source: U.S. Army Field Manual 100-6, "Information Operations," 1996, http://www.fas.org/irp/doddir/army/fm100-6/

2. Martin Libicki writes that information dominance is composed of three elements: "command and control that permits everyone to know where they (and their cohorts) are in the battlespace and enables them to execute operations when and as quickly as necessary; intelligence that ranges from knowing the enemy's dispositions to knowing the location of enemy assets in real-time with sufficient precision for a one-shot kill; and information warfare that confounds enemy information systems at various points (sensors, communications, processing, and command), while protecting one's own. "

Source: *National Defense University Strategic Forum* Number 132, November 1997, http://www.ndu.edu/inss/strforum/SF132/forum132.html

### Information Environment

1. Aggregate of individuals, organizations, or systems that collect, process, or disseminate information, also included is the information itself.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

2. (DOD) The aggregate of individuals, organizations or systems that collect, process, or disseminate information; also included is the information itself.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

3. The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

Source: DoD. *Information Operations*. JP 3-13, February 13 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

### Information Exploitation

The process of extracting, synthesizing, and/or presenting relevant information from vast repositories of raw and structured data. Data includes multiple media and genre types in all the human languages and that also contains geospatial and abstract data. More specifically, Information Exploitation provides the core functionality to access information necessary for an analytic process, especially in the Intelligence Community (IC). At a minimum, Information Exploitation includes: Content Data Transformation, Content Data Mark-up, Information Retrieval, Information Discovery, Analytic Knowledge-Bases, Information Understanding, Assessment and Interpretation, Synthesis and Fusion, and Presentation and Visualization. ARDA's Information Exploitation programs are attempting to significantly advance the state of the art in some of these areas with the expectation that advanced analytic tools will emerge.

Source: Advanced Research Development Agency (ARDA), [See the Wayback Machine, http://tinyurl.com/yjlzb9t ]

### Information Exploitation Office

The Information Exploitation Office (IXO) develops technologies for sensing, exploitation, command/control, and information integration.

Source: DARPA. [See the Wayback Machine, http://tinyurl.com/ykxtxec ]

### Information Fratricide

The results of employing information operations elements in a way that causes effects in the information environment that impede the conduct of friendly operations or cause adverse effects on friendly forces.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

### Information Feudalism

The transfer of knowledge assets from the intellectual commons into private hands. These hands belong to media conglomerates and integrated life sciences corporations rather than individual scientists and authors. The effect of this…is to raise levels of private monopolistic power to dangerous global heights, at a time when states, which have been weakened by the forces of globalization, have less capacity to protect their citizens from the consequences of the exercise of this power.

Source: Peter Drahos, and John Braithwaite. *Information Feudalism: Who Owns the Knowledge Economy?* New York: The New Press, 2003. 2-3.

**Information Function**
Any activity involving the acquisition, transmission, storage, or transformation of information.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995,
[See the Wayback Machine, http://tinyurl.com/ydvgypl ]

**Information Fusion**
***See Information Warfare, Information Warrior***
The ultimate goal of command, control, communications, and computer systems is to produce a picture of the battlespace that is accurate and meets the needs of warfighters. This goal is achieved by fusing i.e., reducing information to the minimum essentials and putting it in a form that people can act on. There is no one fusing of information that meets the needs of all warriors. However, with concise, accurate, timely, and relevant information, unity of effort is improved, and uncertainty is reduced, enabling the force as a whole to exploit opportunities and fight smarter.

Source: Joint Chiefs of Staff. *Joint Doctrine Encyclopedia*. July 16, 1997,
http://www.dtic.mil/doctrine/joint_doctrine_encyclopedia.htm

**Information Gathering and Analysis**
The specific actions taken to gain information about a system element or critical acquisition process for which the level of knowledge is insufficient to permit an informed decision to be made with respect to other risk-handling options.

Source: Defense Acquisition University. *Glossary: Defense Acquisition Acronyms and Terms.* 11th ed.,
2003, http://www.dau.mil/pubs/Glossary/preface.asp

**Information Grid**
***See Information Warfare, Information Warrior, Infosphere***
The networks that result from open systems architectures are called information grids. They allow the warrior users to gain access, process, and transport information in near real time to anyone else on the network. Information grids refer to computer controlled networks that provide virtual connectivity on the demand of the networks that provide virtual connectivity on the demand of the warrior; they support local and area network operations. They are also the basic components of larger grid networks that, when interconnected, support regional, theater, and ultimately a global grid that is also referred to as the infosphere.

Source: Joint Chiefs of Staff. *Joint Doctrine Encyclopedia*. July 16, 1997,
http://www.dtic.mil/doctrine/joint_doctrine_encyclopedia.htm

### Information Laundering

***See Blowback***

Positing rumors or gossip, which would then be picked up by the mainstream broadcast and print media as legitimate stories.

Source: D.J. Peterson. *Russia and the Information Revolution*. Rand National Security Research Division, 2005. 84, http://www.rand.org/pubs/monographs/2005/RAND_MG422.pdf

### Information Life Cycle

Step 1: Created and produced (by authors in all agencies, in all branches, at all levels, and in many different formats and mediums).

Step 2: Cataloged and indexed (metadata tools applied).

Step 3: Temporary and permanent availability and entitlement established (ownership and disclosure rights of creators, publishers, disseminators, licensees, franchisees).

Step 4: Published in the public domain or withheld from disclosure pursuant to a wide variety of statutes, internal agency policies, foreign agreements, and so forth.

Step 5: Put into files, databases, collections, holdings, and other storage repositories.

Step 6: Communicated, disseminated, and distributed.

Step 7: Searched for and retrieved (full text, abstracts, key words). Step 8: Used for decision-making and problem solving.

Step 9: Archived.

Step 10: Re-used over and over again by government officials, journalists, archivists, researchers, citizens, and others (information recycled).

Step 11: Disposed of (temporarily or permanently).

Step 12: Expunged or destroyed if permanent retention period exceeded.

Step 13: Need for new information to replace old information established.

Source: F. Woody Horton. "Government Information Life Cycle Management." Appendix 16 *Comprehensive Assessment of Public Information Dissemination*. National Commission on Libraries and Information Science, June 2000 - March 2001. SUDOC: Y 3.L 61:2 D 63/V.1-4

2. Stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Source: OMB. "Management of Federal Information Resources." Circular A-130. February 1996, http://www.whitehouse.gov/omb/circulars/a130/a130.html

**Information Management**

The provision of relevant information to the right person at the right time in a usable form to facilitate situational understanding and decisionmaking. It uses procedures and information systems to collect, process, store, display, and disseminate information.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Information Operations (IO)**

***See Prepackaged News***

1. Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Source: Defense Acquisition University. *Glossary: Defense Acquisition Acronyms and Terms.* 11th ed., 2003, http://www.dau.mil/pubs/Glossary/preface.asp

2. Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995, [See the Wayback Machine, http://tinyurl.com/ydvgypl ]

3. (DOD) Actions taken to affect adversary information and information systems while defending one's own information and information systems. (Army) The employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect and defend information and information systems and to influence decisionmaking.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

4. The integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to

influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

Source: DoD. *Information Operations*. JP 3-13, February 13 2006. p. iii. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf ; EWA Information and Infrastructure Technologies, Inc. (IIT).http://www.ewa-iit.com/content.asp?sectionID=2 ; National Security Archive. "Rumsfeld's Roadmap to Propaganda: Information Operations Roadmap." January 26, 2006. p.11, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/ and Clay Wilson. "Information Operations and Cyberwar: Capabilities and Related Policy Issues." CRS Report to Congress Updated September 14, 2006, http://www.fas.org/sgp/crs/natsec/RL31787.pdf

### Information Operations Roadmap

***See Prepackaged News, Propaganda, Psychological Operations (PSYOPS), Public Diplomacy***

Obtained under the Freedom of Information Act by the National Security Archive at George Washington University and posted on the Web today, the 74-page "Information Operations Roadmap" admits that "information intended for foreign audiences, including public diplomacy and PSYOP, increasingly is consumed by our domestic audience and vice-versa," but argues that "the distinction between foreign and domestic audiences becomes more a question of USG [U.S. government] intent rather than information dissemination practices."[42]

Source: National Security Archive. "Rumsfeld's Roadmap to Propaganda: Information Operations Roadmap." January 26, 2006. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/ and http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf

### Information Operations Task Force

***See Information Operations Roadmap, Office of Strategic Influence, Public Diplomacy***

Created shortly after September 11, was to focus on "developing, coordinating, deconflicting, and monitoring the delivery of timely, relevant, and effective messages to targeted international audiences."

Source: Daniel Schulman. "Mind Games." *Columbia Journalism Review* May-June 2006, http://www.cjr.org/editorial/mind_games_cjr_on_the_military.php

### Information Owner

An official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

---

[42] Sentiment akin to Walter Lippmann's 1922 idea posited in *Public Opinion* that information and propaganda are indecipherable, and followed up by Jacques Ellul in his various works on propaganda.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

## Information Peacekeeping

1. Information Peacekeeping is the active exploitation of information and information technology--in order to modify peacefully the balance of power between specific individual and groups--so as to achieve national policy objectives. The three elements of Information Peacekeeping, in order of priority, are: open-source intelligence (providing useful actionable unclassified information); information technology (providing "tools for truth" that afford the recipient access to international information and the ability to communicate with others); and electronic security and counter-intelligence (a strictly defensive aspect of Information Operations).

Although Information Peacekeeping is not to be confused with clandestine or covert methods, there are gray areas. Information Peacekeeping may require the clandestine delivery of classified or open source intelligence, or the covert delivery of "tools for truth" such as the traditional radio broadcast equipment, or the more recently popular cellular telephones and facsimile machines. Information Peacekeeping may also require covert assistance in establishing and practicing electronic security and counterintelligence in the face of host country censorship or interference.

Source: Robert D. Steele. "Information Peacekeeping: The Purest Form of War." http://www.fas.org/irp/eprint/cyberwar-chapter.htm

2. A neglected aspect of information operations. Consists of three aspects: open source intelligence, information technology, electronic security and counterintelligence.

Source: Robert D. Steele. *On Intelligence: Spies and Secrecy in an Open World*. Fairfax, VA: AFCEA 2000.

## Information Pollution

The disguising of commercial message sources as editorial. To address the information pollution that may occur when single ads are formatted to resemble stories,

Source: C.T. Cameron and Patricia Curtin, "Tracing sources of information pollution: A survey and experimental test of print media's labeling policy for feature advertising." *Journalism and Mass Communication Quarterly* 71 no.1 (1995): 178-189.

## Information Protection

Security of information and command, control, communications, and computer (C4) systems involves the procedural and technical protection of information and C4 systems major components (terminal devices, transmission media, switches, and control and management), and is an integral component of the joint force commander's command and control protection effort.

Source: Joint Chiefs of Staff. *Joint Doctrine Encyclopedia*. July 16, 1997, http://www.dtic.mil/doctrine/joint_doctrine_encyclopedia.htm

**Information Purification Directives**

***See Propaganda***

"We have created, for the first time in all history, a garden of pure ideology. Where each worker may bloom secure from the pests of contradictory and confusing truths…"

Source: Apple, "1984" Macintosh commercial, http://www.uriahcarpenter.info/1984.html

**Information Requirements**

(DOD, NATO) Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander. (Army) All information elements the commander and staff require to successfully conduct operations, that is, all elements necessary to address the factors of METT-TC. [Note: the Marine Corps uses METT-T].

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Information Resources**

Information and related resources,such as personnel, equipment, funds, and information technology.

Source: "Public Printing and Documents." 44 U.S.C. 3502 (6), http://www.gpoaccess.gov/uscode/browse.html

**Information Resources Management (IRM)**

The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by Agencies. The term includes the management of information and related resources, such as Federal information processing resources.

Information resources management planning is an integral part of overall mission planning. Agencies need to plan from the outset for the steps in the information life cycle. When creating or collecting information, agencies must plan how they will process and transmit the information, how they will use it, how they will protect its integrity, what provisions they will make for access to it, whether and how they will disseminate it, how they will store and retrieve it, and finally, how the information will ultimately be disposed of.

Source: OMB. "Management of Federal Information Resources." Circular A-130. February 1996, http://www.whitehouse.gov/omb/circulars/a130/a130.html

### Information Richness

The richness, or quality, of information has eight attributes that measure important elements of information richness and are displayed on a Kiviat diagram. As discussed earlier, the attributes of information quality that have been in use for decades comprise the majority of those included in Figure 42, specifically:
Information completeness,
Information correctness,
Information currency,
Information accuracy or precision, and
Information consistency.

Source: David S. Alberts, et al, *Understanding Information Age Warfare* , DoD CCRP, August 2001, p. 95-96, http://www.dodccrp.org/files/Alberts_UIAW.pdf

### Information Security

1. Protection of unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Source: U.S. Army Field Manual 100-6, "Information Operations," 1996, http://www.fas.org/irp/doddir/army/fm100-6/

2. Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (C) availability,

which means ensuring timely and reliable access to and use of information; and (D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access/

Source: "Public Printing and Documents." 44 U.S.C. 35 Subchapter II § 3532, http://www.gpoaccess.gov/U.S.C.ode/

3. (DOD) The protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

### Information Security Oversight Office

An agency within the National Archives and Records Administration (NARA), the Information Security Oversight Office (ISOO), which develops security classification policies (including classifying, declassifying and safeguarding national security information for information generated within the federal government and industry, including the National Industrial Security Program (NISP) ; ISOO receives its policy and program guidance from the National Security Council. ISOO evaluates the effectiveness of the security classification programs established by government and industry to protect information vital to "national security interests. " ISOO authority rests with Executive Orders 12958 "Classified National Security Information" [PDF] and 12829 "National Industrial Security Program" [PDF], as amended.

Source: ISOO, http://www.archives.gov/isoo/about/ and ISOO *Annual Reports to the President* http://www.archives.gov/isoo/reports/

### Information Sharing

The term information "sharing" suggests that the federal government entity that collects the information "owns" it and can decide whether or not to "share" it with others. This concept is deeply embedded in the Intelligence Community's culture. We reject it.

Information collected by the Intelligence Community--or for that matter, any government agency--belongs to the U.S. government. Officials are fiduciaries who hold the information in trust for the nation. They do not have authority to withhold or distribute it except as such authority is delegated by the President or provided by law. As we have noted elsewhere, we

think that the Director of National Intelligence could take an important, symbolic first step toward changing the Intelligence Community's culture by jettisoning the term “information sharing” itself--perhaps in favor of the term “information integration” or “information access.”

Source: Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (“Silberman-Robb Commission”). March 31, 2005, http://www.gpoaccess.gov/wmd/index.html

**Information Sharing and Analysis Organization (ISAO)**

Any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

(1) Gathering and analyzing CII in order to better understand security problems and interdependencies related to critical infrastructure and protected systems in order to ensure the availability, integrity, and reliability thereof; (2) Communicating or sharing CII to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to critical infrastructure or protected systems; and (3) Voluntarily disseminating CII to its members, Federal, State, and local governments, or to any other entities that may be of assistance in carrying out the purposes specified in this section.

Source: Department of Homeland Security. “Protected Critical Infrastructure Information.” 6 CFR 29.2, http://www.gpoaccess.gov/cfr/index.html

**Information Sharing Council**

***See Information Sharing Environment***

The Information Sharing Council shall serve during the two-year period beginning on the date of the initial designation of the program manager by the President under subsection (f)(1), unless sooner removed from service and replaced by the President (at the sole discretion of the President) with a successor body.

(2) SPECIFIC DUTIES- In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall-

> (A) advise the President and the program manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE; (B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the ISE; (C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources

to support the ISE; (D) identify gaps, if any, between existing technologies, programs and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment; (E) recommend solutions to address any gaps identified under subparagraph (D); (F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments; and (G) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.

Source: Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638, http://thomas.loc.gov/cgi-bin/query/D?c108:4:./temp/~c108LGI8Vk::

**Information Sharing Environment (ISE)**

***See Sensitive But Unclassified***

1. The terms `information sharing environment' and `ISE' mean an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section.

Source: Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638, http://thomas.loc.gov/cgi-bin/query/D?c108:4:./temp/~c108LGI8Vk::

2. Information Sharing Guidelines. Consistent with section 1016(d) of IRTPA, I hereby issue the following guidelines and related requirements, the implementation of which shall be conducted in consultation with, and with support from, the PM as directed by the DNI:

a. Guideline 1 - Define Common Standards for How Information is Acquired, Accessed, Shared, and Used Within the ISE; b. Guideline 2 - Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector; c. Guideline 3 - Standardize Procedures for Sensitive But Unclassified Information

3. Promoting a Culture of Information Sharing. Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.

Source: Whitehouse Press Release. "Guidelines and Requirements in Support of the Information Sharing Environment." December 16, 2005, http://www.fas.org/sgp/news/2005/12/wh121605-memo.html

and Thomas E. McNamara, "Building on the Information Sharing Environment: Addressing Challenges of Implementation" Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment House Committee on Homeland Security May 10, 2006, http://www.fas.org/irp/congress/2006_hr/051006mcnamara.pdf

3. Creating the ISE is not about building a massive new information system. The ISE aligns and leverages existing information sharing policies, business processes, technologies, systems, and promotes a culture of information sharing through increased collaboration.

Guideline One: The President directed that common standards be developed "to maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE, consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities." These common standards, the President further directed, must accommodate and account for the need to improve upon the sharing of terrorism-related information with State, local, and tribal governments and the private sector.

Source: ISE, http://www.ise.gov/pages/vision.html and http://www.ise.gov/pages/background.html

### Information Silo Affect

Information "silo affect," by which agencies across the federal and state levels fail to share information with each other. The 9/11 Commission cited silo effect as a contributing factor to the failure of U.S. intelligence and law enforcement agencies to track down the terrorists involved in the 9/11 attacks.

Source: OMBWatch "Intelligence Agencies Go Wiki," November 7, 2006, http://www.ombwatch.org/article/articleview/3634/1/1?TopicID=1

### Information Superiority

1. Capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (DoD Directive DoDI 5000.2)

Source: Defense Acquisition University. *Glossary: Defense Acquisition Acronyms and Terms.* 11th ed., 2003, http://www.dau.mil/pubs/Glossary/preface.asp

2. (DOD) That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (Army) The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Also called IS.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

3. That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (JP 1-02). The Air Force prefers to cast `superiority' as a state of relative advantage, not a capability, and views information superiority as: [The degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.] (AFDD 2-5) {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

Source: U.S. Air Force. Public Affairs Operations. Air Force Doctrine Document 2-5.3, June 24, 2005, [See the Wayback Machine, http://web.archive.org/web/20061007174450/http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5.3/afdd2-5.3.pdf ]

**Information System (IS)** [43]

1. A discrete set of information resources (e.g., personnel, data, software, computers, and communications equipment) organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

Source: Defense Acquisition University. *Glossary: Defense Acquisition Acronyms and Terms.* 11th ed., 2003, http://www.dau.mil/pubs/Glossary/preface.asp

2. (Army) The equipment and facilities that collect, process, store, display, and disseminate information. This includes computers—hardware and software—and communications, as well as policies and procedures for their use.

Source: Department of the Army, "Knowledge Management Section," U.S. Army Field Manual 6-01.1, August 29, 2008, http://www.fas.org/irp/doddir/army/fm6-01-1.pdf

---

[43] A list of DoD and intelligence information systems can be found at Federation of American Scientists, http://www.fas.org/irp/program/list.htm; also see William Arkin's "NSA's Multi-Billion Dollar Data Mining Effort." *Washington Post* May 12, 2006, http://blog.washingtonpost.com/earlywarning/2006/05/nsas_multibillion_dollar_data.html

3. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Source: "Public Printing and Documents." 44 U.S.C. 3502 (8), http://www.gpoaccess.gov/uscode/browse.html

4. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (Army) The equipment and facilities that collect, process, store, display, and disseminate information. This includes computers—hardware and software—and communications, as well as policies and procedures for their use. Also called INFOSYS.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Information Technology Agreement (ITA)**

A WTO agreement to eliminate tariffs on a wide range of information technology products. The Information Technology Agreement was concluded at the first ministerial conference of the World Trade Organization at Singapore in December 1996. ITA product coverage includes computers and computer equipment, semiconductors and integrated circuits, computer software products, telecommunications equipment, semiconductor manufacturing equipment, and computer-based analytical instruments. ITA participants were to eliminate tariffs on these products by the year 2000, recognizing that extended staging might be granted in limited circumstances.

Source: Merritt R. Blakeslee and Carlos A. Garcia, *The Language of Trade* 3rd edition, 2001 Department of State, International Information Programs, http://www.4uth.gov.ua/usa/english/trade/language/index.htm

**Information Warfare (IW)**

***See Cyberwar, Defensive Information Warfare, Direct Information Warfare, Netwar, Strategic Information Warfare***

1. Simply the use of information to achieve our national objectives.

Source: George J. Stein. "Information Warfare." [See the Wayback Machine, http://web.archive.org/web/20070311222533/http://www.airpower.maxwell.af.mil/airchronicles/apj/stein.html ]

2. Gone are the terms information-in-warfare and information warfare as they relate to the pillars of IO. Replacing them are three distinct groups of capabilities that form the

foundation of the new doctrinal definition of IO and, when linked, can achieve operationally significant effects: "Information operations . . . are the integrated employment of the capabilities of influence operations, electronic warfare [EW] operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

Source: Capt Randy Mize, USAF "Revised Air Force Doctrine Document 2-5, Information Operations." [See the Wayback Machine, http://web.archive.org/web/20060617215224/http://www.airpower.maxwell.af.mil/airchronicles/apj/apj05/sum05/notam1.html ]

3. Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information based processes, information systems, and computer-based networks.

Source: Defense Acquisition University. *Glossary: Defense Acquisition Acronyms and Terms.* 11th ed., 2003. http://www.dau.mil/pubs/Glossary/preface.asp; Also see: "What is Information Warfare?" National Defense University ACIS Paper 3, August 1995. http://stinet.dtic.mil/cgibin/GetTRDoc?AD=ADA367662&Location=U2&doc=GetTRDoc.pdf

4. Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995, [See the Wayback Machine, http://web.archive.org/web/20040901091302/http://www.af.mil/lib/corner.html]

5. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/ term removed from Joint Doctrine; see DoD. *Information Operations*. JP 3-13, February 13 2006. p. iii, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

6. Any discussion of information warfare, netwar, cyberwar, or even perception manipulation as a component of command and control warfare by the armed forces of the United States at the strategic level must occur in the context of the moral nature of

communication in a pluralistic, secular, democratic society. That is, the question must be raised whether using the techniques of information warfare at the strategic level is compatible with American purposes and principles.

Source: George Stein. "Information War – Cyberwar – Netwar." Battlefield of the Future: 21st Century Warfare Issues." *Air and Space Power Chronicle* [See the Wayback Machine, http://web.archive.org/web/20071110080055/http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html ]

7. In the field of information warfare, everything is, then hypothetical; and just as information and disinformation have become indistinguishable from each other, so have attacks and mere accidents…And yet the message here is not *scrambled,* as was still the case with the counter-measures in electronic warfare; it has become cybernetic. That is to say, the 'information' is not so much the explicit content as the rapidity of its feedback.

Source: Paul Virilio. *The Information Bomb*. Trans., Chris Turner. New York: Verso, 2000. 142-143.

8. Information warfare (IW) - also known as 'infowar' - is a term used to describe any range of attempts by one side in a conflict to deny or disrupt an enemy's information and information systems, while preventing adversaries from doing the same to the information and information systems of friendly forces. IW is a central component of the much broader Revolution in Military Affairs (RMA) currently transforming the US military, and is closely associated with related concepts such as: cyberwar, netwar, command and control warfare (C2W), information operations (IO); as well as older staples of US information strategy such as public diplomacy, psychological operations (PYSOPS), signals intelligence (SIGINT), and electronic warfare (EW).

Source: Konstantin Kilibarda, "Defining Information Warfare (IW)" *Information Warfare Monitor*, http://tinyurl.com/npvry7

**Information Warrior**

***See Information Fusion, Information Grid, Information Warfare***

A new breed of soldier called an information warrior be created within the military. This soldier would be a part of an Information Corps that would "promote jointness where it is critically needed (information interoperability), elevate information as an element of war, develop an information warrior ethos and curriculum, and heighten DOD attention to the global civilian net" (Libicki 1994). Martin C. Libicki (1995) writes "this brave new soldier would not only be sent into the information battlefield, but would also be involved in intelligence-based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace."

Source: Martin Libicki, "The Mesh and the Net: Speculations on Armed Conflict in an Age of Free Silicon." National Defense University, March 1994. [See the Wayback Machine, http://web.archive.org/web/20020203103852/http://www.ndu.edu/ndu/inss/macnair/mcnair28/m028cont.html ] ] and "What is Information Warfare?" National Defense University ACIS Paper 3, August 1995, http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662&Location=U2&doc=GetTRDoc.pdf

**Informational In-Breeding**

***See Information Bureaucratization***

Information secrecy programs, including those implemented by the Department of Defense (DOD), the Department of Energy (DOE), and other federal and state agencies with classified national security responsibilities, create insular "island-like" societies. A sea of requirements, including security clearances 1 and "need to know" 2 restrictions, isolate people outside the "secret island." People with classified information can discuss such information only with persons on their island--those with similar security clearances. 3 This phenomenon creates informational in-breeding, as information can be shared only with the other persons who possess proper security clearances and who have been deemed to have a "need to know." Because of the manner in which bureaucracies award clearances, individuals selected for these programs tend to have predominantly the same background, interests, and values.

Source: Laurent R. Hourcle. "Military Secrecy and Environmental Compliance." *New York University Law Journal* 2 no. 2 (1993), http://www1.law.nyu.edu/journals/envtllaw/issues/vol2/index.html

**Informed Compliance**

The concepts of "informed compliance" and "shared responsibility" were introduced into the Tariff Act of 1930, and the Title VI of the North American Free Trade Agreement Implementation Act (NAFTA). Under Section 484 of the Tariff Act, as amended, 19 U.S.C. Section 1484, it is up to the importer of record to ensure "reasonable care to enter, classify and value imported merchandise, and provide any other information necessary to enable Customs to

properly assess duties, collect accurate statistics and determine whether any other applicable legal requirement is met."

Source: "Entry of Merchandise." 19 U.S.C. Section 1484, http://www.gpoaccess.gov/uscode/browse.html

**Informed Consent**

1. Basic elements of informed consent. In seeking informed consent, the following information shall be provided to each subject:

(1) A statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures which are experimental; (2) A description of any reasonably foreseeable risks or discomforts to the subject. [continues]

Source: "Protection of Human Subjects." 21 CFR 50.2, http://www.gpoaccess.gov/cfr/index.html

2. …in his April 30 letter to Stafford Warren, [Carroll] Wilson announced that the AEC had approved Warren's committee's recommendations for a "program for obtaining medical data of interest to the Commission in the course of treatment of patients, which may involve clinical testing." Wilson's letter spelled out ground rules that were agreed upon. The commission understood that "treatment (which may involve clinical testing) will be administered to a patient only when there is expectation that it may have therapeutic effect." In addition, the commission adopted the requirement for documentation of consent agreed upon in Warren's meeting with the lawyers:

> [I]t should be susceptible of proof from official records that, prior to treatment, each individual patient, being in an understanding state of mind, was clearly informed of the nature of the treatment and its possible effects, and expressed his willingness to receive the treatment.

The commission deferred to Warren's request that written releases from the patient not be required. However,

> it does request that in every case at least two doctors should certify in writing (made part of an official record) to the patient's understanding state of mind, to the explanation furnished him, and to his willingness to accept the treatment.[11]

Source: Department of Energy Openness Project. Advisory Committee on Human Radiation Experiments. (Wilson's use of informed (consent) is one of the earliest uses of the term), http://www.eh.doe.gov/ohre/roadmap/achre/chap1_2.html

3. Respect for persons requires that subjects, to the degree that they are capable, be given the opportunity to choose what shall or shall not happen to them. This opportunity is provided when adequate standards for informed consent are satisfied. While the importance of informed consent is unquestioned, controversy prevails over the nature and possibility of an informed consent. Nonetheless, there is widespread agreement that the consent process can be analyzed as containing three elements: information, comprehension and voluntariness.

*Information*. Most codes of research establish specific items for disclosure intended to assure that subjects are given sufficient information. These items generally include: the research procedure, their purposes, risks and anticipated benefits, alternative procedures (where therapy is involved), and a statement offering the subject the opportunity to ask questions and to withdraw at any time from the research. Additional items have been proposed, including how subjects are selected, the person responsible for the research, etc.

Source: The National Commission for the Protection Of Human Subjects of Biomedical and Behavioral Research. "Ethical Principles and Guidelines for the Protection of Human Subjects of Research." ("Belmont Report"), April 18, 1979, http://www.fda.gov/oc/ohrt/IRBS/belmont.html

### Infosphere

The *Infosphere* is cyberspace ("global systems of internetted computers, communications infrastructure, online conferencing entities, databases and information utilities generally known as the Net"), and a "fifth dimension" of war which have been traditionally fought on land, air, sea. Space control of the infosphere is defined as the ability to use the infosphere for the furtherance of strategic objectives and the ability of the enemy from doing the same.

Source: John Arquilla, and David Ronfeldt. *The Emergence of Noopolitik: Toward an American Information Strategy*. Santa Monica, CA: Rand, 1999, http://www.rand.org/publications/MR/MR1033/

### Infragard

***See Sensitive But Unclassified Information***

An information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the Federal Bureau of Investigation and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories.

Source: Infragard, http://www.infragard.net/, Matthew Rothschild's "The FBI Deputizes Business," March 2008, http://www.progressive.org/mag_rothschild0308 (This story is #3 on the 2009 Project Censored

list), and Matthew Rothschild, "Will NorthCom take over in Swine Flu Outbreak?" *The Progressive* April 29, 2009, http://www.progressive.org/wx042909.html

Each FBI Field Office has a Special Agent Coordinator who gathers interested individuals to form a chapter. Any individual can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited. The following illustrates additional activities that local chapters may offer.

The InfraGard secure website provides members with information about recent intrusions, research related to critical infrastructure protection, and the capability to communicate securely with other members.

Membership Benefits:

- FBI certified and accredited system
- Access to sensitive but unclassified information
- Valuable networking opportunities
- Secure communication

Source: Infragard, "About," http://www.infragard.net/about.php?mn=1&sm=1-0

**In-Q-Tel**

Chartered in 1999 as a private, independent, nonprofit corporation, In-Q-Tel is an evolving blend of corporate strategic venture capital, business, nonprofit and government R&D models. To achieve its mission of identifying and delivering new technologies to the CIA and Intelligence Community (IC), In-Q-Tel borrows key elements from each model that enable it to link the IC to innovation in the commercial market, and back again.

Source: In-Q-Tel. "About IQT," http://www.iqt.org/about-iqt/history.html and https://www.cia.gov/library/publications/additional-publications/in-q-tel/index.html ; also see Melissa Boyle Mahle. *Denial and Deception: an Insider's View of the CIA from Iran-Contra to 9/11*. New York: Nation Books. 267-268.

**Insight Smart Discovery**

***See Data Mining***

Defense Intelligence Agency; Will be a data mining knowledge discovery tool to work against unstructured text. Will categorize nouns (names, locations, events) and present information in images;
Purpose: Analyzing intelligence and detecting terrorist activities;

Status: Planned;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html and J. Nicholas Hoover. "Can Data Mining Catch Terrorists?" *Information Week* May 22, 2006, http://www.informationweek.com/security/showArticle.jhtml?articleID=188100750

**Inspectable Space**

***See TEMPEST***

Three dimensional space surrounding equipment that process classified and/or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and/or remove a potential TEMPEST exploitation exists.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Institutional Controls (IC)**

1. A non-engineered administrative or legal controls that limit land or resource use and/or protect the integrity of a remedy. access or use of property. There are four categories of ICs: governmental controls, proprietary controls, enforcement and permit tools with IC components, and informational devices.

Informational devices include: deed notices, hazardous waste site registries, advisories, and public education activities. Weaknesses: Do not restrict land [exposure] in any way.

Source: Environmental Protection Agency. RCRA National Meeting. "What Are Institutional Controls?" January 16, 2002, http://www.epa.gov/superfund/policy/ic/guide/citguide.pdf

2. Under DOE P 454.1 "institutional controls" may include administrative or legal controls, physical barriers or markers, and methods to preserve information and data and inform current and future generations of hazards and risks.

Source: Department of Energy. Institutional Controls: Implementation Guide. DOE G 454.1-1 10-14-05, http://www.directives.doe.gov/pdfs/doe/doetext/neword/454/g4541-1.pdf

**Instruments of National Power**
All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational and military.

Source: DOD. *DoD Dictionary of Military and Associated Terms*. Joint Publication 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**Integral File Block**
***See File Series***
A distinct component of a file series, as (defined by EO 13292), that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or range of time such as a presidential administration or a five-year retirement schedule within a specific file series that is retired from active use as a group.

Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

**Integrity (of information)**
1. Integrity refers to keeping information accurate, i.e., keeping it from being modified or corrupted.

Source: General Accounting Office (GAO). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. GAO/AIMD-96-84, 1996), http://www.gao.gov

2. "Integrity" refers to the security of information -- protection of the information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification.

Source: Office of Management and Budget (OMB). "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies. " October 1, 2001, http://www.whitehouse.gov/omb/fedreg/final_information_quality_guidelines.html

3. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered or destroyed.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html and Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and

Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

**Intelink**

1. The Intelink-SBU is a US Government, Joint-use, remotely accessed, and operationally implemented information service that is used to access and process unclassified, publicly accessible information only. It provides a protected environment to exchange authorized unclassified, unclassified for official use only, and sensitive but unclassified information among personnel of the Defense, the Diplomatic, the Homeland Security, the Intelligence, and the Law Enforcement communities. The Intelink-SBU firewalls protect users and allow customers to access the public Internet; thus giving Intelink-SBU users a single point of access to an unprecedented amount of unclassified open source information.

Source: DoD, Open Source Intelligence, FMI 2-22.9, Appendix F, December 2006, Expires December 2008, http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf

2. Intelink, which began test bed operation in 1994, is both an architectural framework and an integrated intelligence dissemination and collaboration service providing uniform methods for exchanging intelligence among intelligence providers and users. The Intelink framework conforms to the future direction of the National Information Infrastructure (NII). The Intelink service was patterned after the Internet model in which a variety of institutions have come together in the context of a global network to share information. The IntelLINK intelligence network links information in the various classified databases of the US intelligence agencies (e.g. FBI, CIA, DEA, NSA, USSS, NRO) to facilitates communication and the sharing of documents and other resources.

Source: Globalsecurity.org. "Intelink." http://www.globalsecurity.org/intell/systems/intelink.htm

**Intelligence**

*See Intelligence Information*

1. A body of information and the conclusions drawn there from that is acquired and furnished in response to the known or perceived requirements of customers; it is often derived from information that may be concealed or not intended to be available for use by the acquirer; it is the product of a cyclical process.

A term to refer collectively to the function, activities, or organizations that are involved in the process of planning, gathering, and analyzing information of potential value to decision-makers and to the productions of intelligence as defined in A. above.

The product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of all collected information.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas, and 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

See also acoustic intelligence; all-source intelligence; basic intelligence; civil defense intelligence; combat intelligence; communications intelligence; critical intelligence; current intelligence; departmental intelligence; domestic intelligence; electronic intelligence; electro-optical intelligence; foreign intelligence; foreign instrumentation signals intelligence; general military intelligence; human resources intelligence; imagery intelligence; joint intelligence; laser intelligence; measurement and signature intelligence; medical intelligence; merchant intelligence; military intelligence; national intelligence; nuclear intelligence; open-source intelligence; operational intelligence; photographic intelligence; political intelligence; radar intelligence; radiation intelligence; scientific and technical intelligence; security intelligence; strategic intelligence; tactical intelligence; target intelligence; technical intelligence; technical operational intelligence; terrain intelligence; unintentional radiation intelligence.

[NOTE: the above intelligence types are not entirely listed in this work; they are included to illustrate the level of specialization]

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/data/i/02719.html

3. The technical term of governments to describe all the necessary information, both overt and secret, which it needs for fashioning its policies and doing its work.

Source: Carl J. Friedrich. *The Pathology of Politics: Violence, Betrayal, Corruption, Secrecy, and Propaganda*. New York: Harper & Row, 1972. 210.

4. One of the broadest definitions of intelligence is that "intelligence is knowledge, organization, and activity."10 Arguably, one of the most meaningful purposes of intelligence is "to establish where the danger lies."11 Some would argue based on this definition that "intelligence is intelligence"—that is, differentiating traditional from non-traditional intelligence

is a theoretical matter which may have little relation to the end result—protecting national security. (p.3)

Source: Mark A, Randol, "Homeland Security Intelligence: Perceptions, Statutory Definitions and Counter-Terrorism," *CRS Report for Congress* January 14, 2009, RL33616, http://www.fas.org/sgp/crs/intel/RL33616.pdf

5. Intelligence can be thought of as that which states do in secret to support their efforts to mitigate, influence, or merely understand other nations (or various enemies) that could harm them.

Intelligence thus by definition resist scholarship.

Source: Michael Warner, "Sources and methods for the study of intelligence," *Handbook of Intelligence Studies* Loch Johnson (ed), New York: Routledge, 2007. 17-27.

6. Finally, the real purpose of intelligence - truth telling - must be placed at the center of (*si*c CIA) Agency concerns. This is a harsh prescription; it is certainly the most difficult objective of the lot. But it must be the principal purpose of Agency leadership to establish beyond question the capacity of its experts and its facilities to seek out and find the truth, or the nearest approximation of the truth possible. Public cynicism will have to be dispelled before this is possible; it will take time. (642)

Source: E. Drexel Godfrey Jr. "Ethics and Intelligence." *Foreign Affairs* 56 no.3 (1978):624-642.

### Intelligence Activity

An activity that an agency within the Intelligence Community is authorized to conduct pursuant to the Order.

Source: Department of State. 22 CFR 9. Appendix A, http://www.gpoaccess.gov/cfr/index.html

### Intelligence Committees*

As part of the National Security Act, Congress in 1991 required the Director of Central Intelligence and the heads of all departments, agencies, and other entities of the U.S. government involved in intelligence activities to keep the intelligence committees "fully and currently informed of all intelligence activities," other than a covert action. The procedures for covert actions are spelled out elsewhere. The Intelligence Committees are to receive "any information or material concerning intelligence activities . . . which is requested by either of the intelligence committees in order to carry out its authorized responsibilities

(*House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence)

Source: Louis Fisher, "Congressional Access to Executive Branch Information: Legislative Tools," *CRS Report to Congress May* 17, 2001 RL30966, http://www.opencrs.com

## Intelligence Community

***See In-Q-Tel***

1. The IC is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. These activities include:

- Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;
- Production and dissemination of intelligence;
- Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the US, international terrorist and international narcotics activities, and other hostile activities directed against the US by foreign powers, organizations, persons, and their agents;
- Special activities;
- Administrative and support activities within the US and abroad necessary for the performance of authorized activities; and
- Such other intelligence activities as the President may direct from time to time.

Members of the IC are: Central Intelligence Agency (CIA); within the DoD, the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA), the Defense Intelligence Agency (DIA; State Department's Bureau of Intelligence and Research (INR); Federal Bureau of Investigation (FBI); intelligence organizations of the four military services (Air Force, Army, Navy, and Marines); Department of Homeland Security (DHS); Coast Guard, now part of DHS; Energy Department and Department of the Treasury.

Source: United State Intelligence Community. http://www.intelligence.gov/1who.shtml, Executive Order 12333, "United States Intelligence Activities" http://www.archives.gov/federal-register/executive-orders/1981-reagan.html, and National Intelligence Reform Act of 2004, (S.2845), http://thomas.loc.gov/cgi-bin/query/F?c108:1:./temp/~c108YGu9x6:e8145:

2. The IC as we know it today is the result of half a century of ad hoc development. Each agency or organization makes sense on its own, but if one were to design an IC today from scratch, this is not likely to be the array that would be chosen. Only intelligence, of all major government functions, is carried out by a very disparate number of agencies and organizations that are either independent of one another or housed in separate departments headed by officials whose main concerns are policy, not intelligence. Indeed, referring to it as a "community" is more accurate than most people realize, capturing as it does a sense of mutuality and independence.

Source: United States. Congress. House. Permanent Select Committee on Intelligence. *IC21, Intelligence Community in the 21st Century: Staff Study* (Permanent Select Committee on Intelligence, House of Representatives, One Hundred Fourth Congress Washington: GPO, 1996), http://www.access.gpo.gov/congress/house/intel/ic21/ic21001.html and Terence O'Hara. "In-Q-Tel, CIA's Venture Arm, Invests in Secrets." *Washington Post* August 15, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/14/AR2005081401108.html

## Intelligence Community Directives

The Director of National Intelligence (DNI) established Intelligence Community Directives (ICDs) as the principal means by which the DNI provides guidance, policy, and direction to the Intelligence Community. The DNI also directed that all Director of Central Intelligence Directives (D.C.IDs) remain in force until canceled or superseded by an ICD. The contents of an ICD may be issued in an Intelligence Community Policy Memorandum prior to its formal publication in an ICD.

Source: FAS. "Director of National Intelligence Intelligence Community Directives." http://www.fas.org/irp/dni/icd/index.html

## Intelligence Cycle

***See Intelligence, Intelligence Levels***

1. The process by which information is acquired and converted into intelligence and made available to customers.

Source: Central Intelligence Agency. Office of Public Affairs. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C.: Springfield, VA: National Technical Information Service, [1999?]. SUDOC: PREX 3.2: C 76 and PREX 3.2/2: G 94.

2. Loch K. Johnson characterizes the intelligence cycle as a "funnel of causality," which encompasses a feedback system of personalities, events, history, cycles, ideologies, myths, knowledge, perceptions and experience.

Source: Loch K. Johnson. *America's Secret Power: the CIA at Home and Abroad.* New York: Oxford University Press, 1989. 78-79.

3. The process of tasking, collecting, processing, analyzing, and disseminating intelligence is called the intelligence cycle. The intelligence cycle drives the day-to-day activities of the Intelligence Community. It starts with the needs of those who are often referred to within the Intelligence Community as intelligence "consumers"--that is, policymakers, military officials, and other decision makers who need intelligence information in conducting their duties and responsibilities. These needs--also referred to as intelligence requirements--are sorted and prioritized within the Intelligence Community, and are used to drive the collection activities of the members of the Intelligence Community that collect intelligence. Once information has been collected it is processed, initially evaluated, and reported to both consumers and so-called "all-source" intelligence analysts at agencies like the CIA, DIA, and the State Department's Bureau of Intelligence and Research. All-source analysts are responsible for performing a more thorough evaluation and assessment of the collected information by integrating the data obtained from a variety of collection agencies and sources--both classified and unclassified. This assessment leads to a finished intelligence report being disseminated to the consumer. The "feedback" part of the cycle assesses the degree to which the finished intelligence addresses the needs of the intelligence consumer and will determine if further collection and analysis is required.

Source: Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("Silberman-Robb Commission"). March 31, 2005. and Appendix C. "An Intelligence Community Primer." http://www.gpoaccess.gov/wmd/index.html

**Intelligence Information**

***See Intelligence, Intelligence Cycle, Intelligence Levels***

1. Information that is under the jurisdiction and control of the Director of Central Intelligence or a member of the Intelligence Community.
Information on intelligence community protective security programs (e.g., personnel, physical, technical, and information security).

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995,
http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. Intelligence Information includes the following classified information:

- Foreign intelligence and counterintelligence as defined in EO 12333;

- Information describing U.S. foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained for exploitation; and photography or recordings resulting from U.S. intelligence collection efforts; and
- Information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security). This type of information is collected, processed, produced or disseminated by the Director of Central Intelligence and other agencies of the Intelligence Community under the authority of EO 12333).

Also "Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding."

Several types of intelligence:

- 1. COMINT - Communications intelligence; COMINT is technical and intelligence information derived from foreign communications by other than the intended recipients. COMINT is produced by the collection and processing of foreign communications passed by electromagnetic means, with specific exceptions stated below, and by the processing of foreign encrypted communications, however transmitted. Collection comprises search, intercept, and direction finding. Processing comprises range estimation, transmitter/operator analysis, traffic analysis, cryptanalysts, decryption, study of plain text, the fusion of these processes, and the reporting of results. COMINT shall not include:

> Intercept and processing of unencrypted written communications, except the processing of written plain text versions of communications which have been encrypted or are intended for subsequent encryption.
>
> Intercept and processing of press, propaganda and other public broadcasts, except for processing encrypted or "hidden meaning" passages in such broadcasts.
>
> Oral and wire interceptions conducted under DoD Directive 5200.24.
>
> Censorship.

2. Information from the intercept of foreign communications by other than the intended recipients; it does not include the monitoring of foreign public media or the intercept of communications obtained during the course of counterintelligence investigations within the United States. COMINT includes the fields of traffic analysis, cryptanalysis, and direction finding, and is a part of Signals Intelligence (SIGINT).

Source: Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C.: Springfield, VA: National Technical Information Service, [1999?]. SUDOC: PREX 3.2: C 76 PREX 3.2/2: G 94.

## Types of Intelligence

ELINT - Electronics intelligence; ELINT is technical and intelligence information derived from foreign, non-communications, electromagnetic radiations emanating from other than atomic detonation or radioactive sources. ELINT is produced by the collection (observation and recording), and the processing for subsequent intelligence purposes of that information.

GEOINT - (DOD) The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. Also called GEOINT.

Source: *DoD Dictionary of Military and Associated Terms*. Joint Publication 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/ and NGA, Office of GEOINT Sciences, http://earth-info.nga.mil/GandG/

HUMINT - Human based intelligence
A DOD and NATO term: A category of intelligence derived from information collected and provided by human sources. [Note: in Army and Marine Corps usage, human intelligence operations cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations.]

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

IMINT - Imagery intelligence.

MASINT - Measurement and Signatures Intelligence.

MEDINT - Medical Intelligence
That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in

both military and civilian sectors.

OSINT - Open-source intelligence; Information of potential intelligence value that is available to the general public.

RINT - Unintentional Radiation Intelligence. Intelligence derived from the collection and analysis of non-information bearing elements extracted from the electromagnetic energy unintentionally emanated by foreign devices, equipment, and systems, excluding those generated by the detonation of nuclear weapons.

Source: Joint Chiefs of Staff. *Joint Doctrine Encyclopedia*. July 16, 1997, http://www.dtic.mil/doctrine/joint_doctrine_encyclopedia.htm

SIGINT - Signals communications, electronics, and foreign instrumentation signals
A category of intelligence information comprising all Communications Intelligence (COMINT), Electronics Intelligence (ELINT), and Telemetry Intelligence (TELINT). SIGINT operational control is the authoritative direction of SIGINT activities, including tasking and allocation of effort, and the authoritative prescription of those uniform techniques and standards by which SIGINT information is collected, processed and reported.

TECHINT - Technical intelligence. Refers chiefly to IMINT and SIGINT.

TELENT - Technical and intelligence information derived from the intercept, processing, and analysis of foreign telemetry.

Source: Defense Security Service [See the Wayback Machine, http://web.archive.org/web/20061214152720/http://www.dss.mil/isec/chapter9.htm ], DoD. *DoD Dictionary of Military Terms and Associated Terms*, JP-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/ and DODD 5100.20. "The National Security Agency and the Central Security Service," December 23, 1971, ASD (I), thru Ch 4, June 24, 1991, http://www.fas.org/irp/doddir/dod/d5100_20.htm

**Intelligence Information Report**
Intelligence Information Report (IIR). The IIR is the primary vehicle to provide human intelligence information to the consumer. It uses a message format structure which supports automated data entry into Intelligence Community databases.

Source: DoD. "DoD Counterintelligence Collection Reporting." DoD 5240.17. October 26, 2005, http://www.dtic.mil/whs/directives/corres/pdf/i524017_102605/i524017p.pdf

**Intelligence Journal**

A chronological log of intelligence activities covering a stated period, usually 24 hours. It is an index of reports and messages that have been received and transmitted, important events that have occurred, and actions taken. The journal is a permanent and official record.

Source: Department of Defense. DoD *Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**Intelligence Levels | Levels of Intelligence**

***See Intelligence, Intelligence Cycle***

The levels of intelligence correspond to the established levels of war: **strategic, operational,** and **tactical.** Like the levels of war, the levels of intelligence serve as a framework in which commanders and MI personnel visualize the logical flow of operations, allocation of resources, and assignment of tasks. The levels of intelligence are not tied to specific echelons but rather to the intended outcome of the operations which they support. As illustrated in Figure 2-1, echelons and levels of intelligence vary. The relationship is based upon the political and military objectives of the operation and the commander's needs.

Source: Department of the Army. FM 34-1. "Fundamental of IEW Operations." Chapter 2. *Intelligence and Electronic Warfare Operations*. September 1994.

http://www.fas.org/irp/doddir/army/fm34-1/ch2.htm#2-6

**Intelligence Method**

The method which is used to provide support to an intelligence source or operation, and which, if disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in supporting the foreign intelligence or foreign counterintelligence activities of the United States, or which would, if disclosed, reasonably lead to the disclosure of an intelligence source or operation.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/

**Intelligence Oversight Board (IOB)**

***See President's Foreign Intelligence Advisory Board***

1. Established as a standing committee of the President's Foreign Intelligence Advisory Board (PFIAB). The IOB shall consist of no more than four members designated by the President from among the membership of the PFIAB. The Chairman of the PFIAB may also serve as the Chairman or a member of the IOB if so designated by the President. The IOB shall utilize such full-time staff and consultants as authorized by the Chairman of the IOB with the concurrence

of the Chairman of the PFIAB. Sec. 2.2. The IOB shall:

(a) prepare for the President reports of intelligence activities that the IOB believes may be unlawful or contrary to Executive order or Presidential directive; (b) forward to the Attorney General reports received concerning intelligence activities that the IOB believes may be unlawful or contrary to Executive order or Presidential directive; (c) review the internal guidelines of each agency within the Intelligence Community that concern the lawfulness of intelligence activities; (d) review the practices and procedures of the Inspectors General and General Counsel of the Intelligence Community for discovering and reporting intelligence activities that may be unlawful or contrary to Executive order or Presidential directive; and (e) conduct such investigations as the IOB deems necessary to carry out its functions under this order.

Source: "War and National Defense." 50 U.S.C. 15 § 401.http://www.gpoaccess.gov/cfr/index.html

2. The President's Intelligence Oversight Board (IOB) was established by President Gerald Ford in 1976 as a White House entity with oversight responsibility for the legality and propriety of intelligence activities. The Board, which reports to the President, is charged primarily with preparing reports "of intelligence activities that the IOB believes may be unlawful or contrary to Executive order or Presidential directive." The Board may also refer such reports to the Attorney General. This standard assists the President in ensuring that highly sensitive intelligence activities comply with law and Presidential directive. In 1993, the IOB was made a standing committee of the PFIAB.

Source: Central Intelligence Agency. "Executive Oversight of Intelligence." *Factbook on Intelligence.* [See the Wayback Machine, http://web.archive.org/web/20060616234124/http://cia.gov/cia/publications/facttell/executive_oversight.html ]

3. An independent oversight board created to identify intelligence abuses after the CIA scandals of the 1970s did not send any reports to the attorney general of legal violations during the first 5 1/2 years of the Bush administration's counterterrorism effort, the Justice Department has told Congress.

Source: John Solomon "Intelligence World, a Mute Watchdog: Panel Reported No Violations for Five Years," *Washington Post* July 15, 2007; for oversight, see Department Of Justice Corrective Actions on the FBI's Use of National Security Letters, March 20,2007, http://www.justice.gov/opa/pr/2007/March/07_nsd_168.html

4. Executive Order 13462 established the President's Intelligence Advisory Board who also serve on the "IOB shall consist of not more than five members of the PIAB who are designated by the President from among members of the PIAB…" (5.b)

Source: G.W. Bush, EO 13462, February 29, 2008, http://edocket.access.gpo.gov/2008/pdf/08-970.pdf

**Intelligence Process**
The process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. See also analysis and production; collection; dissemination and integration; evaluation and feedback; intelligence; planning and direction; processing and exploitation.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Intelligence Report (INTREP)**
A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information.

Source: Department of Defense Dictionary. *DoD of Military and Associated Terms*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Intelligence Reporting**
The preparation and conveyance of information by any means.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Intelligence SAP**
***See Special Access Program***
A SAP [Special Access Program] primarily to protect the planning and execution of especially sensitive intelligence or CI operations or collection activities.

Source: Department of the Army. "Special Access Programs (SAPs) and Sensitive Activities." AR 380-381. April 21, 2004. http://www.fas.org/irp/doddir/army/ar380-381.pdf

**Intelligence Subject Code**
A system of subject and area references to index the information contained in intelligence reports as required by a general intelligence document reference service.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Intelligence, Surveillance and Reconnaissance (ISR)**
The term "intelligence, surveillance and reconnaissance," or "ISR," encompasses multiple activities related to the planning and operation of sensors and assets that collect, process, and disseminate data in support of current and future military operations. Intelligence data can take many forms, including optical, radar, or infrared images or electronic signals. This data can come from a variety of sources, including surveillance and reconnaissance systems ranging from satellites, to manned aircraft like the U-2, unmanned aircraft systems like the Air Force's Global Hawk and Predator and the Army's Hunter, to other ground, air, sea, or space-based equipment, to human intelligence teams. DOD ISR activities support the missions of the Department of Defense and the Director of National Intelligence, as well as the missions of other government agencies.

Source: Testimony, Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives, *Preliminary Observations on DOD's Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development*, GAO April 19, 2007. http://www.gao.gov

**Intellipedia**
[Classified] wiki for the Intelligence Community
Lives on the Joint Worldwide Intelligence Communications System (JWICS)

Source: FAS. DNI press release http://www.fas.org/irp/news/2006/10/odni103006.pdf

**Interagency Security Classification Appeals Panel (ISCAP)**
An agency within the National Archives and Records Administration (NARA) which provides the "public and users of the classification system with a forum for further review of classification decisions." Established by Executive Order 12958 "Classified National Security Information," signed on April 17, 1995. ISCAP's mission under EO 12958 § 5.3:

1. Classification Challenges: deciding on appeals by authorized persons who have filed classification challenges under Section 1.8 of EO 12958, as amended;
2. Exemptions from Automatic Declassification: approving, denying or amending agency exemptions from automatic declassification, as provided in Section 3.3 of EO 12958, as amended; and

3. Mandatory Declassification Review Appeals: deciding on mandatory declassification review appeals by parties whose requests for declassification under Section 3.5 of EO 12958, as amended, have been denied at the agency level.

ISCAP is composed of representatives of the Departments of Defense, State and Justice, the CIA, NARA and the National Security Adviser.

Source: Interagency Security Classification Appeals Panel (ISCAP). http://www.archives.gov/isoo/oversight-groups/iscap/index.html, Federation of American Scientists http://www.fas.org/sgp/advisory/iscap/ and William Burr, "The Secrecy Court of Last Resort," National Security Archive June 5, 2009, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB276/index.htm

**Internal Affairs Treasury Enforcement Communications System Audit Data Mart**
***See Data Mining***
Department of Homeland Security. Assists the Internal Affairs group by mining criminal activity data to ascertain how Customs' employees are using the Treasury Enforcement System;
Purpose: Detecting criminal activities or patterns;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004. http://www.gao.gov/htext/d04548.html

**International Public Information [IPI] System**
***See Information Operation Roadmap***
30 April 1999 President Clinton issued a secret Presidential Decision Direction -- PDD 68 -- ordering the creation of an International Public Information (IPI) to address problems identified during military missions in Kosovo and Haiti, when no single US agency was empowered to coordinate US efforts to sell its policies and counteract bad press abroad. The IPI system is geared towards prevention and mitigation of crises and operate on a continuous basis. PDD-68 is evidently intended to replace the provisions of NSDD 77 "Management of Public Diplomacy Relative to National Security" issued by President Reagan on 14 February 1983.

International Public Information [IPI] System is designed to "influence foreign audiences" in support of US foreign policy and to counteract propaganda by enemies of the United States. The intent is "to enhance U.S. security, bolster America's economic prosperity and to promote democracy abroad," according to the IPI Core Group Charter.

Source: Presidential Decision Directive PDD 68, 30 April 1999, http://www.fas.org/irp/offdocs/pdd/pdd-68.htm and http://www.fas.org/irp/offdocs/pdd/pdd-68.htm

**Interrogation Operations**

DoD defines intelligence interrogation as the systematic process of using approved interrogation approaches to question a captured or detained person to obtain reliable information to satisfy intelligence requirements, consistent with applicable law. Interrogation is an art that can only be effective if practiced by trained and certified interrogators. Certified interrogators are trained to employ techniques that will convince an uncooperative source to provide accurate and relevant information

Source: DoD, Office of the Inspector General, Report No. 06-INTEL-10 August 25, 2006 Evaluation Report, *Review of DoD-Directed Investigations of Detainee Abuse,* http://www.dodig.mil/Ir/reports/ExecSum_IntelRpt_082506.pdf and United States. Congress. House. Committee on the Judiciary. Subcommittee on the Constitution, Civil Rights, and Civil Liberties. *Department of Justice to Guantanamo Bay: Administration Lawyers and Administration Interrogation Rules. Part I*: hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Committee on the Judiciary, House of Representatives, One Hundred Tenth Congress, second session, May 6, 2008, http://tinyurl.com/ybw66k ]

**Investigative Data Warehouse**

1. The IDW provides the capability to broaden data exploitation for the FBI's intelligence and investigative efforts, to search and present integrated results in a desired form on a single user platform, and also manage the quality of service provided by the FBI and other government agencies. In addition, the IDW allows examination of relationships between items of interest, including persons, places, communications devices, organizations, financial transactions, and case-related information across large amounts of data.

The IDW Program objectives are to:

- Create a data warehouse using consistently defined and implemented data elements to provide a single-access repository for information;
- Consistently define, store, and display varied information (data, text, graphics, drawing, imagery, photos, audio, and video);

Source: FBI, "Investigative Data Warehouse," http://www.fbi.gov/hq/ocio/idw_011209.htm

2. Despite the vast amount of personal information contained in the IDW, the FBI has never published a Privacy Act notice describing the system or explaining the ways in which the records might be used.

Source: Electronic Frontier Foundation, "FOIA: DOJ's Investigative Data Warehouse," http://www.eff.org/issues/foia/061773RBW

3. There are 38 data sources were included in the IDW on or before August 2004.

Source: Electronic Frontier Foundation, "Report on the Investigative Data Warehouse," April 2008, http://www.eff.org/issues/foia/investigative-data-warehouse-report

**ISE Shared Spaces**

a key element of the ISE EAF (*Enterprise Architecture Framework)*—describes a functional concept, not a technology implementation approach. The ISE EAF helps resolve the information processing and usage problems identified by the 9/11 Commission and IRTPA by employing a structured, networked approach to information sharing

Make standardized terrorism-related information, applications and services accessible to other ISE participants in each of the three ISE security domains—SBU, Secret, and Sensitive Compartmented Information (SCI);

Source: ISE, *Annual Report to Congress on the Information Sharing Environment* 2008, http://www.fas.org/irp/agency/ise/2008report.pdf

---

**~ J ~**

**Joint Advertising and Market Research Database**

1. The committee believes that the Department of Defense has an important corporate-level role to play in complementing the recruiting and advertising programs of the individual services. In that light, the committee believes that the Department's joint advertising and market research reinvention effort can have a direct, positive long-term impact on the ability of the Department and the military services to recruit quality personnel. The committee believes that such a capability is especially critical at a time when the recruiting efforts of the military services could soon be challenged by a range of factors. For that reason, the committee recommends an increase of $10.0 million to the budget request for the Department's joint advertising and market research effort.

Source: House Report 108-491, National Defense Authorization Act for Fiscal Year 2005, http://www.thomas.gov/cgi-bin/cpquery

2. In May 2005, the Department of Defense announced that it had created a massive database for recruiting. The "Joint Advertising and Market Research" system proposed to combine student information, Social Security Numbers, and information from state motor vehicle repositories into a mega database of all those 16-25 years of age. The information would be housed at a private direct marketing firm. In June 2005, EPIC and eight privacy and consumer groups objected to the creation of the database, arguing that it violated the Privacy Act and was unnecessarily invasive.

Source: Electronic Privacy Information Center (EPIC) comments to DoD, http://epic.org/privacy/profiling/dodrecruiting.html

**Joint Document Exploitation Center (JDEC)**
A physical location for deriving intelligence information from captured adversary documents including all forms of electronic data and other forms of stored textual and graphic information. It is normally subordinate to the joint force/J-2. See also intelligence.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Joint Information Bureau (JIB)**
Facility established by the joint force commander to serve as the focal point for the interface between the military and the media during the conduct of joint operations. When operated in support of multinational operations, a joint information bureau is called a "combined information bureau" or an "allied press information center."

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Joint Intelligence Community Council**
The National Intelligence Director, who shall chair the Council. Consists of the following:

` (2) The Secretary of State.
` (3) The Secretary of the Treasury.
` (4) The Secretary of Defense.
` (5) The Attorney General.
` (6) The Secretary of Energy.
` (7) The Secretary of Homeland Security.
` (8) Such other officers of the United States Government as the President may designate from time to time.

`(c) FUNCTIONS- The Joint Intelligence Community Council shall assist the National Intelligence Director to in developing and implementing a joint, unified national intelligence effort to protect national security by--

> `(1) advising the Director on establishing requirements, developing budgets, financial management, and monitoring and evaluating the performance of the intelligence community, and on such other matters as the Director may request; and
>
> ` (2) ensuring the timely execution of programs, policies, and directives established or developed by the Director.

Source: U.S. Code, TITLE 50 > CHAPTER 15 > SUBCHAPTER I > § 402-
http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00000402----001-.html

> **Joint Interrogation and Debriefing Center**
>
> A physical location for the exploitation of intelligence information from enemy prisoners of war and other nonprisoner sources. It is normally subordinate to the joint force/J-2.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Joint Military Intelligence Program**

The JMIP shall improve the effectiveness of DoD intelligence activities when those activities involve resources from more than one DoD Component; when users of the intelligence data are from more than one DoD Component; and/or when centralized planning, management, coordination, or oversight will contribute to the effectiveness of the effort. The JMIP shall initially be comprised of the following component programs

(Programs, functions, and activities may be added to or deleted from JMIP, on the approval of the Deputy Secretary of Defense.):

a. Defense Cryptologic Program
b. Defense Imagery Program (DIP).
c. Defense Mapping, Charting, and Geodesy Program (DMCGP).
d. Defense General Intelligence and Applications Program (DGIAP).
   (1) Defense Airborne Reconnaissance Program (DARP).
   (2) Defense Intelligence Counterdrug Program (DICP).
   (3) Defense Intelligence Agency's Tactical Program (DIATP).
   (4) Defense Space Reconnaissance Program (DSRP).
   (5) Defense Intelligence Special Technology Program (DISTP).

Source: DOD Directive 5205.9 Joint Military Intelligence Program (JMIP), April 7, 1995, http://www.fas.org/irp/doddir/dod/jmip.htm and Richard A. Best, Jr. "Intelligence, Surveillance, and Reconnaissance (ISR) Programs: Issues for Congress." *CRS Report to Congress February* 22, 2005, http://www.fas.org/sgp/crs/intel/RL32508.pdf

**Joint Protection Enterprise Network (JPEN)**

***See Data Mining***

1. System Location : Booz-Allen Hamilton, Inc, 5201 Leesburg Pike, Suite 400, Falls Church, VA 22041-3203.

**Categories of individuals covered by the system:** Any individual, civilian or military, involved in, witnessing or suspected of being involved in or reporting possible criminal activity affecting the interests, property, and/or personnel on a DoD installation.

**Categories of records in the system:** Investigative information supporting known or suspected suspicious activity and incidents at DoD installations. Information includes subject's name, aliases, Social Security Number, address(es), telephone number, date of birth, driver's license number, passport number, license plate number, vehicle description, description of occupants, source of investigation, risk analysis, threat assessment, victim names, names of informants, names of law enforcement officers and investigators, and subject's group affiliations, if any.

**Retention and disposal:** Disposition pending (until the National Archives and Records Administration approves the retention and disposition of these records, treat as permanent).

**Authority for maintenance of the system:** 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 8013, Secretary of the Air Force; 10 U.S.C. 5013, Secretary of the Navy; Section 21, Internal Security Act of 1950 (Pub. L. 81-831); 40 U.S.C. 318, as delegated by the Administrator, General Services Administration, to the Deputy Secretary of Defense, September 1987, Special Police; and E.O. 9397 (SSN).

**Record source categories:** Suspects, witnesses, victims, and other personnel, informants, various DoD, federal, state, and local investigative agencies, and any other individual or organization, which may supply pertinent information.

Source: *Federal Register* September 26, 2003 Volume 68 no. 187 pages 55593-55594. http://www.gpoaccess.gov/fr/search.html and DefenseLINK http://www.defenselink.mil/privacy/notices/js/JS008CSD.html

2. Information shared in JPEN includes reports of suspected surveillance of military facilities; elicitation attempts and suspicious questioning; tests of security; unusual repetitive activities; bomb threats; and other suspicious activity. Additionally, JPEN can report incidents

such as chemical, biological, radiological, nuclear alarms or alerts; fire and bomb explosions; vehicle turn-rounds; and force protection conditions. The general noted USNORTHCOM plans to expand JPEN DoD-wide within its area of responsibility over the next two years.

> Management of the JPEN system officially transferred to USNORTHCOM Dec. 5. The command, which declared full operational capability of its homeland defense mission Sept. 11, 2003, now has the responsibility to make the JPEN system operational across the nation.

Source: NORTHCOM. "JPEN Shares Antiterrorism Information Across Nation." March 3, 2004. http://www.northcom.mil/News/2004/030304.html and DoD, Inspector General *Threat and Local Observation Notice (TALON) Report Program* Appendix I. Deputy IG for Intelligence, June 20, 2006, Memorandum, Report No. 07-1 NTEL-09 June 27,2007, http://www.fas.org/irp/agency/dod/talon.pdf

**Joint Psychological Operations Task Force**

***See Psychological Operations***

Composed of headquarters and operational assets. It assists the joint force commander in developing strategic, operational, and tactical psychological operation plans for a theater campaign or other operations. Mission requirements will determine its composition and assigned or attached units to support the joint task force commander. Also called JPOTF. (JP 1-02)

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Joint Regional Information Exchange System (JRIES)**

Began as a pilot project for the sharing of counterterrorism information between local and state law enforcement and the Department of Defense (DOD). JRIES was initiated by the Joint Intelligence Task Force - Combating Terrorism (JITF-CT), led by the Defense Intelligence Agency (DIA). The initial participants included the New York Police Department Counterterrorism Bureau (NYPD-CTB) and the California Department of Justice Anti-Terrorism Information Center (CATIC). After assessment of the pilot phase, JRIES became operational in February 2003. The number of participants has also grown to include other municipalities, states, and federal agencies

Source: Harold C. Relyea and Jeffrey W. Seifert. "Information Sharing for Homeland Security: A Brief Overview." *CRS Report to Congress* January 10, 2005, http://www.fas.org/sgp/crs/RL32597.pdf

**Joint Regional Intelligence Center**[44]

The Joint Regional Intelligence Center, the first such center in the nation, opened its doors Thursday to help more than 2001 law enforcement agencies coordinate their efforts to prevent terrorist attacks.

More than 30 intelligence analysts from the FBI, the Los Angeles Police Department, the Los Angeles County Sheriff's Department and other agencies are already working out of the Norwalk facility. The center will serve as a hub for information gathering, analysis and sharing among federal, state and local law enforcement officials and safety agencies. The aim of the effort is preventing terrorist attacks and combating violent crime in Los Angeles, Orange, Ventura, San Bernardino, Riverside, Santa Barbara and San Luis Obispo counties.

Source: Ashley Surdin. "Intelligence Center for Los Angeles Region Begins Its Work." Los Angeles Times July 28, 2006, http://www.latimes.com/news/local/la-me-homeland28jul28,0,1741923.story?coll=la-home-headlines

**Joint Worldwide Intelligence Communications System (JWICS)**

***See Intellipedia***

The sensitive, compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**JUNE Mail**

In June 1949, Hoover approved the JUNE mail procedure. Whenever reporting information obtained from "highly confidential sources" (i.e., wiretaps, bugs, break-ins, or mail openings) or from "the most sensitive sources, such as Governors, secretaries to high officials who may be discussing such officials and their attitude," FBI agents were to caption these reports "JUNE." Thus captioned, these reports were to be routed to the Special File Room at FBI headquarters to be "maintained under lock and key." Hoover supplemented these restrictions in July 1949 when issuing *Bureau Bulletin* number 34. Whenever uncovering information that "could cause embarrassment to the Bureau, if distributed," agents were not to include this information within the text of their report but instead "on administrative pages attached to the regular report." Officials at FBI headquarters could detach the administrative pages whenever the report was

[44] How does the Joint Regional Intelligence Center mesh with the JTTF (Joint Terrorism Task Force)? [See Bill of Rights Defense Committee "JTTF FAQ," http://www.bordc.org/resources/jttf-faq.php ]

"distributed to agencies outside the Bureau"—and no one would know that information was being withheld.

These reports were then to be maintained separate from the FBI's central records system in a Special File Room at the FBI headquarters in Washington, D.C. FBI Director William Webster terminates the JUNE Mail procedure in November 1978.

Source: Athan Theoharis, ed. *The FBI: A Comprehensive Reference Guide*. Phoenix: Oryx Press, 1998. 31-32, 368.

---

**~K ~**

**Keystone Principle of Classification**

1. Compilations of unclassified information to which the compiler has added no substantive value (i.e., no substantive information) should not be classified. This conclusion is based on a fundamental principle of classification—that classified information cannot be completely subdivided into separate, unclassified components. DOE has stated this principle as follows:

> Information that is classified under the Atomic Energy Act must not be so subdivided that all its components (including contextual information) are unclassified.*

This is sometimes called the *keystone principle of classification*. This keystone principle may be visualized by considering a classified photograph or drawing that has been subdivided into many components (e.g., pieces of a puzzle), each of which reveals an item of information. According to the keystone principle of classification, not all of the components can be unclassified if the entire entity is classified. One or more key pieces must be classified so that the entire "picture" cannot be obtained when all of the unclassified pieces are assembled. Thus, if individual items of information are truly unclassified (i.e., if no classification error has been made), then assembling (compiling) the items cannot reveal classified information. [This rule is stated in several DOE classification guides.]

Source: Arvin S. Quist. "Classification of Compilations of Information." Security Classification of Information. volume 2, chapter 10. April 1993, http://www.fas.org/sgp/library/quist2/chap_10.html

2. Classification of all information of potential use to proliferants or adversaries is impractical and poses an unwarranted burden on the flow of information in a free society. Therefore, a keystone approach, which classifies the minimum amount of key information, critical to the development and production of nuclear weapons, shall be utilized. (Proposed).

Source: Dr. Paul T. Cunningham, Chair. "Appendix G." *Report of the Fundamental Classification Policy Review Group Report of the Nuclear Materials Production Working Group.* January 15, 1997, http://www.fas.org/sgp/library/app-g.html

**Knowledge**

In the context of the cognitive hierarchy, information analyzed to provide meaning and value or evaluated as to implications for the operation.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Knowledge Management**

1. The art of creating, organizing, applying, and transferring knowledge to facilitate situational understanding and decisionmaking. Knowledge management supports improving organizational learning, innovation, and performance. Knowledge management processes ensure that knowledge products and services are relevant, accurate, timely, and useable to commanders and decisionmakers. (FM 3-0)

Source: Department of the Army, "Knowledge Management Section," U.S. Army Field Manual 6-01.1, August 29, 2008, http://www.fas.org/irp/doddir/army/fm6-01-1.pdf

2. Knowledge Management is a set of management practices which has been recently forged out of the combination of organization studies, information science and management practice. While Knowledge Management is still new as a reference discipline, it has already established a formal position in the worlds of management and academia.

Source: Federal Knowledge Management Initiative, "Preliminary Roadmap," Federal KM Working Group, February, 2009, http://wiki.nasa.gov/cm/wiki/?id=6251#gen31

---

## ~ L ~

**Latest Time Information is of Value**

The time by which an intelligence organization or staff must deliver information to the requester in order to provide decisionmakers with timely intelligence. This must include the time anticipated for processing and disseminating that information, as well as for making the decision.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Law Enforcement Information Sharing Program (LEISP) Exchange Specification**
A subset of the National Information Exchange Model (NIEM) — was developed to serve as an "interpreter" between different law enforcement systems, enabling participants on one system to obtain results from others in a familiar format.

At the Federal level, the FBI's Law Enforcement On-line (LEO) system has provided a protected means for sharing Sensitive But Unclassified (SBU) data with regional law enforcement (LE) agency partners through a project originally known as Regional Data Exchange (R-DEx) and subsequently adopted by the Department of Justice (DOJ) for all of its components and renamed OneDOJ. Using LEO, DOJ is integrating the OneDOJ regional partnerships with a new Law Enforcement National Data Exchange (N-DEx) program under the FBI Criminal Justice Information Services (CJIS) Division. In addition, DOJ supports six Regional Information Sharing System (RISS) Network centers that provide tailored support for specialized LE functions to meet regional needs

The LEISP Exchange Specification (LEXS) defines a common format in which law enforcement data can be shared. The most commonly used elements form the foundation upon which practitioners can build specialized extensions to suit individual communities. LEXS 3.1 is based on NIEM 2.0.

Source: Justice Standards Clearinghouse Implementation, http://it.ojp.gov/default.aspx?area=implementationAssistance&page=1017&standard=486

**Law Enforcement Information Sharing Program (LEISP) Exchange Specification (LEXS)**
A subset of the National Information Exchange Model (NIEM)— was developed to serve as an "interpreter" between different law enforcement systems, enabling participants on one system to obtain results from others in a familiar format.

Source: ISE, *Annual Report to Congress on the Information Sharing Environment* 2008, http://www.fas.org/irp/agency/ise/2008report.pdf

**Law Enforcement Sensitive**
***See Controlled Unclassified Information***
Unclassified but should not be disseminated beyond law enforcement circles; provides more detailed information about potential suspects that would be inappropriate to publicize. The FBI

is "moving away from SBU to its own LES." It is not clear if LES is also a type of clearance (p.164 n.184 & p.85 n.118).

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004. http://www.cops.usdoj.gov/default.asp?Item=1404, DOJ, *Law Enforcement Intelligence Classifications, Products and Dissemination*, November 23, 2004, http://www.cops.usdoj.gov/pdf/e09042536_Chapter_06.pdf and "Capitol Police papers found on street," *Washington Times* December 7, 2009, http://www.washingtontimes.com/news/2009/dec/07/capitol-police-papers-found-on-street-corner/

**Leak**

1. A disclosure of information that has been classified under EO 10501.

Source: NARA. Eisenhower EO 10501, November 5, 1953 "Safeguarding Official Information in the Interests of the Defense of the United States," http://www.archives.gov/federal-register/executive-orders/1953-eisenhower.html

2. Administrative Leak. Unauthorized disclosure of administrative matters (Part VII; 4d) Classified Information Security Leak. Deliberative disclosures of classified information (Part B.)

Source: Charles Coolidge, Chairman. *Report to the Secretary of Defense by the Committee on Classified Information*. Department of Defense. November 8, 1956 [45] http://www.thememoryhole.org/foi/coolidge.htm; for an interesting discussion on leaks, see Rep. John E. Moss, Special Subcommittee on Government Information, and Mr. Coolidge, in United States. Congress. House. Committee on Government Operations. Special Subcommittee on Government Information. *Availability of Information from Federal Departments and Agencies.* (Part 8. Department of Defense. Hearings before the United States House Committee on Government Operations, Special Subcommittee on Government Information, Eighty-Fifth Congress, first session, on Mar. 11, 12, 1957. Washington: GPO, 1957, SUDOC: Y4.G 74/7: IN3/pt.8).

3. Coined in the early twentieth century, was applied to inadvertent slips in which information was picked up by reporters. The words quickly acquired a broader, more active meeting: any calculated release of information to reporters with the stipulation that the source remains unidentified.

Source: Richard Kielbowicz. "Leaks to the Press as a Communication within and between Organizations." *Newspaper Research Journal* 1 no. 2 (1979/1980): 53-58 and United States. Congress. Senate. Committee

[45] The Coolidge Committee also recommended in 8c. agencies "give reasons for classification whenever possible when requests for information are denied."

on the Judiciary. *Examining DOJ's investigation of journalists who publish classified information: lessons from the Jack Anderson case*: hearing before the Committee on the Judiciary, United States Senate, One Hundred Ninth Congress, second session, June 6, 2006. Washington: U.S. G.P.O., 2007, http://www.fas.org/irp/congress/2006_hr/journalists.html

4. Hess: Typology of Leaks:

Ego Leak: Giving information primarily to satisfy a sense of self.

Goodwill Leak: Information offered to "accumulate credit" as a play for a future favor.

Policy Leak: A straightforward pitch for or against a proposal using some document or insider information as the lure to get more attention than might be otherwise justified. The leak of the Pentagon Papers falls into this category.

Animus Leak: Used to settle grudges; information is released in order to cause embarrassment to another person.

Trial-Balloon Leak: Revealing a proposal that is under consideration in order to assess its assets and liabilities. Usually proponents have too much invested in a proposal to wan to leave it to the vagaries of the press and public opinion. More likely, those who send up a trial balloon want to see it shot down, and because it is easier to generate opposition to almost anything than to build support, this is the most likely effect.

Whistleblower Leak: Usually used by career personnel; going to the press may be the last resort of frustrated civil servants who feel they cannot resolve their dispute through administrative channels. Hess is careful to point out that Whistleblowing is not synonymous with leaking.

Source: Stephen Hess. *The Government/Press Connection: Press Officers and their Offices.* Washington, D.C.: Brookings Institution, 1984. 77-79; also see John Dean's "Bush's Unofficial Official Secrets Act: How the Justice Department Has Pushed to Criminalize The Disclosure of Non-Security Related Government Information." http://writ.news.findlaw.com/dean/20030926.html

5. Unauthorized disclosures of classified information; a communication or physical transfer of information to an unauthorized recipient.

Source: Department of Defense. DoD Directive 5210.50 July 22, 2005, "Unauthorized Disclosure of Classified Information to the Public." http://www.fas.org/irp/DoDdir/DoD/d5210_50.pdf ; Secretary of Defense Donald Rumsfeld "The Impact of Leaking Classified Information" memo July 12, 2002. http://foi.missouri.edu/whistleblowing/impactofleaking.pdf ; and Dave Eberhart. "CIA Expert: Leaks of Classified Information Must Stop." July 27, 2002. (this article reported James B. Bruce, vice chairman of the DNI/CIA's Foreign Denial and Deception Committee, statement that "We've got to do whatever it takes – if it takes sending SWAT teams into journalists' homes – to stop these leaks." Story archived at The Memory Hole, http://www.thememoryhole.org/cia-swat-journalists.htm)

6. *Unauthorized disclosures of classified information.* As one of the primary bodies intended to conduct oversight of intelligence activities on behalf of the American people, we are mindful of the need for ongoing and thorough review of such activities. However, the delicate balance between protecting national security and safeguarding civil liberties must be carried out in a manner that fully protects both interests, through mechanisms such as regular reporting to the congressional intelligence committees and the use of the Intelligence Community Whistleblower Protection Act. By definition, no individual--whether a journalist, government official, or intelligence community employee--can or should singlehandedly presume to determine what information `deserves' to be withheld from disclosure in order to protect national security, especially without full knowledge of the surrounding context.

Source: House Intelligence Committee report on the FY 2007 Intelligence Authorization Act. FAS, http://www.fas.org/irp/congress/2006_rpt/hrpt109-411.html

7. (U) NSA/CSS shall identify unauthorized media disclosures of classified NSA/CSS information. In accordance with the procedures and responsibilities outlined below, significant media disclosures of NSA/CSS classified information shall be communicated to NSA/CSS organizations, the Department of Defense (DoD), the Director of National Intelligence (DNI), and the Department of Justice (DoJ).

(U) The determination that an unauthorized disclosure qualifies as a significant unauthorized disclosure shall be made by the Office of Policy and Records (D.C.3) and the Office of General Counsel (D2). Organizations with purview over disclosed information shall not make this determination.

(U//FOUO) Information associated with an unauthorized media disclosure shall be classified at the level of the disclosure. Until an actual classification level has been determined, references to potential unauthorized disclosures shall be protected as classified.

(U//FOUO) Indications or assessments of potential damage resulting from an unauthorized disclosure shall not be releasable to foreign countries or international organizations unless specifically directed otherwise by the Director, NSA/Chief, CSS (DIRNSA/CHCSS) or the Director of Policy and Records. Information regarding unauthorized disclosures of intelligence information shall be marked as NOFORN, and transmittal of any information regarding unauthorized disclosures shall employ special protections (e.g., encryption).

Source: NSA/CSS. "Reporting Unauthorized Media Disclosures of Classified NSA/CSS Information." NSA/CSS Policy 1-27, 20 March 2006, http://www.fas.org/irp/nsa/unauthorized.html

8. It should be noted that some high ranking officials erroneously believe they have the authority to leak classified information in furtherance of government policy. Such disclosures may only be made by persons with declassification authority under Executive Order 12065 or otherwise from the President. Without such authority, "friendly" leaks are just as unlawful as any other unauthorized disclosure of classified information.

Source: Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information" (the "Willard" Report), March 31, 1982, http://www.fas.org/sgp/library/willard.pdf

9. In a momentous expansion of the government's authority to regulate public disclosure of national security information, a federal court ruled that even private citizens who do not hold security clearances can be prosecuted for unauthorized receipt and disclosure of classified information.

The August 9 (2006) ruling by Judge T.S. Ellis, III, denied a motion to dismiss the case of two former employees of the American Israel Public Affairs Committee (AIPAC) who were charged under the Espionage Act with illegally receiving and transmitting classified information.

Source: FAS, *Secrecy News*, August 10, 2006, http://www.fas.org/sgp/jud/rosen080906.pdf and http://www.fas.org/blog/secrecy/2006/08/recipients_of_leaks_may_be_pro.html

**Leak Anxiety**

No formal definition, but mentioned in the *Secrecy News* article "Disclosure of TSA Manual Stirs Leak Anxiety," on the release of a "sensitive" TSA passenger screening manual and corresponding congressional inquiries regarding TSA's policy on inadvertent disclosures and leak of agency information to nongovernmental blogs and Web sites.

Source: FAS, "Disclosure of TSA Manual Stirs Leak Anxiety," *Secrecy News* December 10, 2009, http://www.fas.org/blog/secrecy/2009/12/leak_anxiety.html.

**Leveraging**

In information operations, the effective use of information, information systems, and technology to increase the means and synergy in accomplishing information operations strategy

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Library Awareness Program**

Although its FBI code name remains secret (Foerstel 1991: 176), details of the program were first brought to national prominence in a September 18, 1987 front page story in the *New York*

*Times*. From 1973 until the late 1980s, the FBI conducted a secret surveillance program within America's unclassified scientific libraries, including both public and university libraries. That program, known as the Library Awareness Program, had two goals: To restrict access by foreign nationals, particularly Soviet and East Europeans, to unclassified scientific information, and to recruit librarians to report on any "foreigners" using America's unclassified scientific libraries.

The Library Awareness Program seems related to the notorious NSDD-145 "to encourage, advise, assist the private sector" in protecting "sensitive non-government information" (Foerstel 1991: 178)

Source: Herbert N. Foerstel. "Secrecy in Science; Remarks." March 29, 1999. http://www.aaas.org/spp/secrecy/Presents/foerstel.htm and his *Surveillance in the Stacks: the FBI's Library Awareness Program.* New York: Greenwood Press, 1991.

**Limited Access Authorization (LAA)**
Security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring such limited access in the course of their regular duties.

Source: DoD. *National Industrial Security Manual* (NISPOM). DoD 5220.22-M, February 28, 2006. https://www.dss.mil/GW/ShowBinary/DSS/isp/fac_clear/download_nispom.html

**Limited Official Use Information (LOU)**
1. Term used to designate unclassified information of a sensitive, proprietary, or personally private nature that must be protected against release to unauthorized individuals.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. Unclassified information of a sensitive, proprietary, or personally private nature which must be protected against release to unauthorized individuals. Information must not be designated Limited Official Use to conceal inefficiency. misdeeds or mismanagement.

Sensitive unclassified information "shall be identified" as Limited Official Use information. Categories of LOU:

- Informant and witness information
- Grand Jury information
- Investigative information
- Information that could be sold for profit
- Personal information which falls subject to the Privacy Act of 1974

- Reports that disclose security vulnerabilities

Source: U.S. Department of Justice Order 2620.7, September 2, 1987 and U.S. Department of Justice. United States Marshals Service. Office of Inspections. Internal Security Division. *Information Security*. Washington D.C.: 1991. SUDOC: J 25.2: In 3

### Low 2 Information

Internal matters of a relatively trivial nature; records that "are related solely to the internal personnel rules and practices of an agency."

Source: U.S. Department of Justice. Freedom of Information Act Guide, http://www.usdoj.gov/oip/exemption2.htm#low2

---

**~ M ~**

### Magic Lantern

1. Magic Lantern can be remotely installed on a computer via e-mail containing a virus disguised as a harmless computer file, known as a "Trojan horse" program, or through other common vulnerabilities hackers use to break into computers, Keystrokes recorded by Magic Lantern can be stored to be seized later in a raid or even transmitted back to the FBI over the Internet.

Source: Center for Democracy and Technology (CDT). "Digital Search and Seizure: Updating Privacy Protections to Keep Pace with Technology". February 2006, http://www.cdt.org/publications/digital-search-and-seizure.pdf

2. Under the "sneak and peek" provision of the USA Patriot Act, pushed through Congress by John Ashcroft, the FBI, with a warrant, can break into your home and office when you're not there and, on the first trip, look around. They can examine your hard drive, snatch files, and plant the Magic Lantern on your computer. It's also known as the "sniffer keystroke logger." Once installed, the Magic Lantern creates a record of every time you press a key on the computer. It's all saved in plain text, and during the FBI's next secret visit to your home or office, that information is downloaded as the agents also pick up whatever other records and papers they find of interest.

Source: Nat Hentoff. "The FBI's Magic Lantern Ashcroft Can Be in Your Computer" *Village Voice* May 24, 2002, http://www.villagevoice.com/news/0222,hentoff,35142,6.html

**Mandatory Declassification Review (MDR)**

1. Review for possible declassification performed in response to a request received from an organization or an individual.

Source: Defense Intelligence Agency. Office of Security and Counterintelligence, Policy and Security Awareness Branch. *Desk Reference Guide to Executive Order 12958, as Amended, Classified National Security Information.* April 2004.

2. MDR is a means by which any individual can request an agency to review a classified record for declassification, regardless of its age or origin, subject to certain limitations set forth in E.O. 12958, as amended.

Source: Information Security Oversight Office. *2005 Report to the President.*, http://www.archives.gov/isoo/reports/

**Masking**

Masking is the other special type of classification and is the act of classifying one piece of information solely to protect a separate item of information.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

**Material**

An data regardless of physical form or characteristic, including written or printed matter, automated information system storage media, maps, charts, paintings, drawings, film, photographs, engravings, sketches, working notes, papers, reproductions of any such things by any means or process, and sound, voice, magnetic or electronic recordings.

Source: War and National Defense. 50 U.S.C. 15 Subchapter VI § 435a http://www.gpoaccess.gov/uscode/browse.html, and the Permanent House Select Committee on Intelligence. S. 2507 "To authorize appropriations for fiscal year 2001 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes." http://www.fas.org/irp/congress/2000_rpt/s2507.html

**Matrix (Multistate Anti-Terrorism Information Exchange)**

***See Data Mining***

Matrix was operated by the data-aggregator company Seisint ("provider of information management products"), purchased by Lexis Nexis in September 2004. Matrix database information included commercial and government information such as vehicular records,

professional and hunting licenses, voter rolls, and court records, available to law enforcement officials to track potential terrorist activity.

Discontinued in April 2005, Matrix II is currently being discussed in Florida with plans to enlarge the scope of information to financial and insurance records.

Source: ACLU. "Feature on MATRIX." http://www.aclu.org/Privacy/Privacy.cfm?ID=14240&c=130 and Ryan Singel. "Florida Planning Son of Matrix." *Wired* April 25, 2005, http://www.wired.com/news/privacy/0,1848,67313,00.html and Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview" Updated January 18, 2007, http://opencrs.com/document/RL31798/2007-01-18

**Media**

Any print, electronic, or broadcast outlet (including blogs) where information is made available to the general public.

Source: NSA/CSS. "Reporting Unauthorized Media Disclosures of Classified NSA/CSS Information." NSA/CSS Policy 1-27, 20 March 2006, http://www.fas.org/irp/nsa/unauthorized.html

**Media Embed**

2. C. A media embed is defined as a media representative remaining with a unit on an extended basis –perhaps a period of weeks or even months. (2)

3. B Without making commitments to media organizations, deploying units will identify local media for potential embeds and nominate them through PA Channels. (3).

6. A. Media products will not be subject to security review or censorship except as indicated in Para. 6. A.1. Security at the source will be the rule. U.S. military personnel shall protect classified information from unauthorized or inadvertent disclosure. (11)

6.A.1 The nature of the embedding process may involve observation of sensitive information, including troop movements, battle preparations, materiel capabilities and vulnerabilities and other information as listed in Para 4.G. When a commander or his/her designated representative has reason to believe that a media member will have access to this type of sensitive information, prior to allowing such access, he/she will take prudent precautions to ensure the security of that information.

What information is sensitive and what the parameters are for covering this type of information If media are inadvertently exposed to sensitive information they should be briefed after exposure on what information they should avoid covering. (11-12)

Source: Public Affairs Guidance (PAG) on Embedding Media During Possible Future Operations/deployments in the U.S. Central Command (CENTCOM) Area of Responsibility (AOR). February 2003, http://www.defenselink.mil/news/Feb2003/d20030228pag.pdf

**Metadata**

1. Data describing stored data about data; that is, data describing the structure, data elements, interrelationships, and other characteristics of electronic records.

Source: DoD. 5015.2-STD. "Design Criteria Standard for Electronic Records Management Software Applications." http://www.dtic.mil/whs/directives/corres/pdf/50152std_061902/p50152s.pdf

2. Information about information; more specifically, information about the meaning of other data.

Source: DoD. *The Department of Defense Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**METT-TC**

A memory aid used in two contexts: (1) In the context of information management, the major subject categories into which relevant information is grouped for military operations: mission, enemy, terrain and weather, troops and support available, time available, civil considerations. (2) In the context of tactics, the major factors considered during mission analysis. [Note: the Marine Corps uses METT-T: mission, enemy, terrain and weather, troops and support available-time available.]

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Midnight Regulations**

The Bush administration disputed news reports of heightened regulatory activity in its final months. "There's no great increase in the number of regulations that we're reviewing right now," White House spokesman Tony Fratto told the press October 31 about the Office of Management and Budget's customary review of agencies' significant regulations.1
In fact, OMB's Office of Information and Regulatory Affairs, or OIRA, approved 157 final rules from September 1, 2008, to December 31, 2008, according to RegInfo.gov. OIRA approved only 83 final rules during the same period in 2007; 92 in 2006; and 81 in 2005.

This increased output is not uncommon. Most administrations pump out a stream of new regulations at the end of a president's term. These regulations are disparagingly called "midnight" regulations. But not all midnight regulations are created equal. (See Appendix).

Source: Reece Rushing, Rick Melberth, and Matt Madia, *After Midnight: The Bush Legacy of Deregulation and What Obama Can Do,* January 2009, Center for American Progress and OMBWatch, http://www.americanprogress.org/issues/2009/01/after_midnight.html

**Military Analyst Program**

The Pentagon military analyst program was launched in early 2002 by then-Assistant Secretary of Defense for Public Affairs Victoria Clarke. The idea was to recruit "key influentials" to help sell a wary public on "a possible Iraq invasion." Former NBC military analyst Kenneth Allard called the effort "psyops on steroids."

Source: SourceWatch, "Pentagon military analysts program," http://www.sourcewatch.org/index.php?title=Pentagon_military_analyst_program, Bryan Whitman, "Pentagon used psychological operation on US public, documents show," *Raw Story* http://rawstory.com/2009/09/bryan-whitman-part-1/ and DOD Reading Room, "Military Analyst Program", http://www.dod.mil/pubs/foi/milanalysts/

**Military Deception**

***See Deception***

Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are as follows.

a. Strategic military deception--Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations.

b. Operational military deception--Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater to support campaigns and major operations.

c. Tactical military deception--Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements.

d. Service military deception--Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems.

e. Military deception in support of operations security (OPSEC)--Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities.

Source: DoD. *DoD Dictionary of Military and Associated Terms*. Joint Publication 1-02.As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/; DoD. *Military Deception*. Joint Publication 3-13.4 (Formerly JP 3-58) July 13, 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_4.pdf and Clay Wilson. "Information Operations and Cyberwar: Capabilities and Related Policy Issues." CRS Report to Congress Updated September 14, 2006, http://www.fas.org/sgp/crs/natsec/RL31787.pdf

**Military Information Function**
Any information function supporting and enhancing the employment of military forces.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995.
[See the Wayback Machine, http://tinyurl.com/ydvgypl ]

**Military Intelligence Board (MIB)**
A decisionmaking forum which formulates Defense intelligence policy and programming priorities. The Military Intelligence Board, chaired by the Director, Defense Intelligence Agency, who is dual-hatted as Director of Military Intelligence, consists of senior military and civilian intelligence officials of each Service, US Coast Guard, each Combat Support Agency, the Joint Staff/J-2/J-6, Deputy Assistant Secretary of Defense (Intelligence), Intelligence Program Support Group, DIA's Directorates for Intelligence Production, Intelligence Operations, and Information and Services, and the combatant command J-2s.

Source: Department of Defense. *DoD Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/

**Military Intelligence Integrated Data System/Integrated Database (MIIDS)**
An architecture for improving the manner in which military intelligence is analyzed, stored, and disseminated. The Integrated Database (IDB) forms the core automated database for the Military

Intelligence Integrated Data System (MIIDS) program and integrates the data in the installation, order of battle, equipment, and selected electronic warfare and command, control, and communications files. The IDB is the national-level repository for the general military intelligence information available to the entire Department of Defense Intelligence Information System community and maintained by DIA and the commands.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Military Security**

Denial to the enemy during such time as it can be useful to him of all knowledge, that in the opinion of the authority responsible for such military security would benefit him materially.

Source: Louis Nicot Ridenour. "Military Security & the Atomic Bomb." *Fortune* November (1945): 32, 170-171, 216, 218, 221, 223.

**Military Sensemaking | Sensemaking**

1. Sensemaking is a relatively new concept that has largely been associated with Weick (1995) and his work in organizational behavior. Sensemaking refers to the set of processes involved in trying to improve one's understanding of a situation, often in response to surprise. (p. i)

Source: Winston R. Sieck, et al, FOCUS: A Model of Sensemaking, Technical Report 1200 May 2007, http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=A469770&Location=U2&doc=GetTRDoc.pdf; also see Per-Arne Persson and James M. Nyce, *Technology and Sensemaking in the Modern Military Organization*, 7th ICCRTS 2002, http://www.dodccrp.org/events/7th_ICCRTS/Tracks/Track_3.htm (scroll down for article) Sensemaking Symposium, October 23-25, 2001, http://www.dodccrp.org/events/2001_sensemaking_symposium/Day_1.htm and Command and Control Research Program, Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence *Final Report Sensemaking Symposium*, October 23-25, 2001, http://www.au.af.mil/au/awc/awcgate/ccrp/sensemaking_final_report.pdf

2. Sensemaking is the current buzz word in discussions of C2, having succeeded situational awareness (SA) as everybody's favorite concept.[11] As a consequence, sensemaking has come to acquire a variety of meanings but it seems now to be used most often with its everyday, commonsense meaning (with all the outdated philosophical baggage that this implies) rather than with its original technical meaning introduced by Weick (1995) as what people do in order to decide how to act in the situations they encounter. This has made the concept less useful than it could have been.

In the DOODA concept, we follow Weick (1995) and define sensemaking as the function that produces an understanding of the mission in terms of what needs to be done to accomplish it in the situation at hand.

Source: Berndt Brehmer, "Understanding the Functions of C2 Is the Key to Progress," Command and Control Research Program 1 no. 1 (2007), http://www.dodccrp.org/html4/journal_v1n1_07.html

3. Sensemaking is about such things as placement of items into frameworks, comprehending, redressing surprise, constructing meaning, interacting in pursuit of mutual understanding, and patterning.

Source: Karl E. Weick, *Sensemaking in Organizations*, Thousand Oaks: Sage Publications, 1995: 6.

4. Sense-Making mandates the construction of attributes which capture aspects of movement in time-space bound moments to attributes which attend in some way Sense-Making's central concepts: time, space, movement, gap (p.154); Sense-Making, specifically through the use of the Sense-Making metaphor, mandates that attention be focused on the phenomenological horizon of the actor's world – the past (including the historical past), the present, and the future; as well as the connections (verbings) between past-present-future (p. 155). {Sense-Making is variously described as a metaphor and a methodology)

Source: Brenda Dervin, "Sense-Making's Journey from Metatheory to Methodology to Method: An Example using Information Seeking and Use as Research Focus," Brenda Dervin, Lois Foreman-Wernet, and Eric Lauterbach (eds), *Sense-making Methodology Reader: Selected Writings of Brenda Dervin.* (Cresskill, NJ: Hampton Press, 2003: 133-164), http://communication.sbs.ohio-state.edu/sense-making/art/artabsdervin03smjourney.html

5. The process by which individuals (or organizations) create an understanding so that they can act in a principled and informed manner. Sensemaking tasks often involve searching for documents that are relevant for a purpose and then extracting and reformulating information so that it can be used. When a sensemaking task is difficult, sensemakers usually employ external representations to store the information for repeated manipulation and visualization. Sensemaking tasks inherently involve an embodiment as an actor (or actors), an environment, forms of knowing, and ways to work with what is known. Working can take different forms -- such as logical, metaphorical, physical, or image-based reasoning

Source: PARC (Palo Alto Research Center) Glossary, http://www2.parc.com/istl/groups/hdi/sensemaking/gloss-frame.htm

### Military Symbol

A military symbol is a graphic representation of units, equipment, installations, control measures, and other elements relevant to military operations. As a part of doctrine, these symbols provide a common visual language for all users. Standardization of military symbols is essential if operational information is to be passed among military units without misunderstanding.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Minefield Record**

A DoD and NATO term: A complete written record of all pertinent information concerning a minefield, submitted on a standard form by the officer in charge of the laying operations.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Minerva Consortia | Project Minerva**

***See Human Terrain System, Project Camelot***

1. With the Minerva initiative, we envision a consortia of universities that will promote research in specific areas. These consortia could also be repositories of open-source documentary archives. The Department of Defense, perhaps in conjunction with other government agencies, could provide the funding for these projects.

Let me be clear that the key principle of all components of the Minerva Consortia will be complete openness and rigid adherence to academic freedom and integrity. There will be no room for "sensitive but unclassified," or other such restrictions in this project. We are interested in furthering our knowledge of these issues and in soliciting diverse points of view – regardless of whether those views are critical of the Department's efforts. Too many mistakes have been made over the years because our government and military did not understand – or even seek to understand – the countries or cultures we were dealing with.

Source: Robert Gates, Address to the Association of American Universities, Washington, D.C., April 14, 2008, http://www.defenselink.mil/speeches/speech.aspx?speechid=1228

2. When research that could be funded by neutral civilian agencies is instead funded by the military, knowledge is subtly militarized and bent in the way a tree is bent by a prevailing wind. The public comes to accept that basic academic research on religion and violence "belongs" to the military; scholars who never saw themselves as doing military research now do; maybe they wonder if their access to future funding is best secured by not criticizing U.S.

foreign policy; a discipline whose independence from military and corporate funding fueled the kind of critical thinking a democracy needs is now compromised; and the priorities of the military further define the basic terms of public and academic debate.

Source: Hugh Gusterson, "The U.S. military's quest to weaponize culture," *Bulletin of the Atomic Scientists* June 20, 2008, http://www.thebulletin.org/web-edition/columnists/hugh-gusterson/the-us-militarys-quest-to-weaponize-culture

**Misinformation**

***See Disinformation***

1. Incorrect information from any source that is released for unknown reasons or to solicit a response or interest from a non-political or non-military target.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

2. Misinformation refers to false or misleading information that is spread unintentionally. If one unwittingly spreads false or misleading information, that is misinformation. Of course, many times it is impossible to ascertain intentions, so it may not be clear whether false information represents disinformation or misinformation. Misinformation can be further subdivided into:

**Media Mistakes** which happen frequently given the pressure of deadlines and imperfect knowledge

**Urban Legends** -- Untrue stories that are widely believed because they speak to a widespread fear, hope, or other emotion

**Conspiracy Theories** -- Belief that powerful, evil hidden forces are secretly manipulating the course of world events and history.

Source: U.S. State Department. International Information Programs. "How to Identify Misinformation." http://usinfo.state.gov/media/Archive/2005/Jul/27-595713.html [See the Wayback Machine, http://web.archive.org/web/20080115092101/http://usinfo.state.gov/media/Archive/2005/Jul/27-595713.html ]

3. The Second Circuit U.S. Court of Appeals recently ruled that the U.S. Environmental Protection Agency (EPA) is not liable for any harm resulting from their intentional misinformation about air quality around the World Trade Center (WTC) site following the

September 11 attacks. The lawsuit, *Lombardi v. Whitman*, was filed by five emergency responders who worked at the WTC site without adequate safeguards, in part because of the misguided assurances of safe air quality. The April 19 court decision favors protecting government liability over the public's right to know about environmental risks that could compromise their safety.

Source: OMBWatch, "Court Picks Illusion of Safety over Protecting Public," May 1, 2007, http://www.ombwatch.org/article/articleview/3819/1/1?TopicID=1

**Mission Creep**

1. Mission creep is one the leading risks of data mining cited by civil libertarians, and represents how control over one's information can be a tenuous proposition. Mission creep refers to the use of data for purposes other than that for which the data was originally collected. This can occur regardless of whether the data was provided voluntarily by the individual or was collected through other means.

Source: Jeffrey W. Seifert. "Data Mining: An Overview." *CRS Report for Congress* January 27, 2006, http://www.fas.org/sgp/crs/secrecy/RS20748.pdf

2. In the decade of the 1990s the term mission creep became a buzzword. Even though its precise meaning is uncertain, mission creep influences military operations on the policy, operational, and tactical common definition produced a trump card that levels. ..One definition of mission creep is derived from situations in which the military moves from well-defined or achievable missions to ill-defined or impossible ones. This implies setting up forces for failure since missions become unachievable.

Source: Adam B. Siegel. "Mission Creep or Mission Understood?" http://www.dtic.mil/doctrine/jel/jfq_pubs/1825.pdf

**Model Counterterrorism Investigative Strategy (MCIS)**

On November 18, 2002 the Foreign Intelligence Surveillance Court of Review issued an opinion approving the Intelligence Sharing Procedures, thereby authorizing the FBI to share information, including FISA-derived information, between our criminal and intelligence investigations. With this opinion, we were finally able to conduct our terrorism investigations with the full use and coordination of our criminal and intelligence tools and personnel. (U)

To formalize this merger of intelligence and criminal operations, we have abandoned the separate case classifications for "criminal" international terrorism investigations (with the classification number 265) and "intelligence" international terrorism investigations

(classification number 199), and have consolidated them into a single classification for "international terrorism" (new classification number 315). This reclassification officially designates an international terrorism investigation as one that can employ intelligence tools as well as criminal processes and procedures. In July 2003, we formalized this approach in our Model Counterterrorism Investigative Strategy (MCIS), which was issued to all field offices and has been the subject of extensive field training. (U)

Source. Department of Justice. FBI Response to "A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks." June 2005, http://www.usdoj.gov/oig/special/0506/app3.htm and CBSnews.com "New FBI Intel Rules Worry Critics." http://www.cbsnews.com/stories/2003/12/13/terror/main588380.shtml

**Modernized Integrated Database (MIDB)**
The national level repository for the general military intelligence available to the entire Department of Defense Intelligence Information System community and, through Global Command and Control System integrated imagery and intelligence, to tactical units. This data is maintained and updated by the Defense Intelligence Agency. Commands and Services are delegated responsibility to maintain their portion of the database. (JP 3-51)

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Modus Operandi Database**
*See Data Mining*
Department of the Air Force. Is an investigative tool used to identify and track trends in criminal behavior. It links characteristics of crimes and provides details on crime scenes and other crime factors;
Purpose: Detecting criminal activities or patterns;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: No.

[**Note from Maret**, p.31 of the GAO report: one expects a system of this nature from let's say, DOJ, but the Air Force? Is this a clerical error on GAO's part? FOIA researchers, help!]

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Mosaic Theory**

1. Also termed *compilation theory*. Under the Freedom of Information Act, an agency is required to disclose any information that does not fall within one of the FOIA exemptions. However, some information, while seemingly innocuous or suitable for public release on its own, can be extremely harmful when grouped with other information. To provide protection from public disclosure of information that merits protection because of the context in which it is presented, the courts have sanctioned the use of the "mosaic" or "compilation" theory. The compilation approach is explicitly recognized in Executive Order 12958, supra, which sets forth the standards for applying compilation in classifying national security information.

> Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. "Compilation" means an aggregation of pre-existing unclassified items of information. Section 1.7(e) of E.O. 12958, as amended by E.O. 13292 or March 25, 2003, 68 FR 15,315 (March 28, 2003).

The courts have applied the theory most commonly in the national security area, where the courts have repeatedly stated that the "mosaic-like nature of intelligence gathering" often changes the way an agency will classify or protect information that seems otherwise innocuous. *Salisbury v. U.S.,* 690 F. 2d 966, 971 (D.C. Cir. 1982). However, its use also has been routinely sanctioned for withholding information under exemptions other than Exemption 1. *See, e.g.*, *Dorsett v. Dept. of Treasury*, 307 F. Supp 2d 28 (D.D.C. 2004) (Exemption 2), *Halperin v. CIA*, 629 F. 2d 144 (D.C. Cir. 1980) (Exemption 3); *Timken Co. v. U.S. Customs Service*, 491 F. Supp 557 (D.D.C. 1980) (Exemption 4); *Center for National Security Studies v. U.S. Department of Justice*, 331 F. 3d 918 (D.C. Cir. 2003) (Exemption 7).

Source: Nuclear Regulatory Commission. *Task Force Report on Public Disclosure of Security-Related Information*. SECY-05-0091. May 18, 2005, http://www.fas.org/sgp/othergov/nrc-disc.pdf

2. Within the government these systems process and communicate classified national security information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this serious damage to the United States and its national security interests.

Source: Reagan National Security Decision Directive Number 145. "National Policy on Telecommunications and Automated Information Systems Security." http://www.fas.org/irp/offdocs/nsdd145.htm

3. Describes a basic precept of intelligence gathering. Disparate items of information, though individually of limited or no utility to the possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts. In the context of national security, the mosaic theory suggests the potential for an adversary to deduce from independently innocuous facts a strategic vulnerability, exploitable for malevolent ends.

Source: David Pozen. "The Mosaic Theory, National Security, and the Freedom of Information Act." *Yale Law Journal* 115 no. 3 (2005): 102, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=820326

4. Even using the Government's theoretical model of a mosaic, it must be acknowledged that the mosaic theory is only as persuasive as the tiles which compose it and the glue which binds them together -- just as a brick wall is only as strong as the individual bricks which support it and the cement that keeps the bricks in place. Therefore, if the individual pieces of a mosaic are inherently flawed or do not fit together, then the mosaic will split apart, just as the brick wall will collapse. A final point must be kept in mind. One consequence of using intelligence reports and summaries in lieu of direct evidence is that certain questions simply cannot be answered, i.e., there are no [*16] witnesses to cross-examine or deposition transcripts to consult. 4 Sizeable gaps may appear in the record and may well remain unfilled; each party will attempt to account for these deficiencies by positing what they think are the most compelling logical inferences to be drawn from the existing evidence. Accordingly, that existing evidence must be weighed and evaluated as to its strength, its reliability, and the degree to which it is corroborated

Source: *All Ali Bin Ali Ahmed, et al v. Barack H. Obama,* , et al., Respondents, United States District Court for the District of Columbia, Civil Action No. 05-1678, May 11, 2009; also see Andy Worthington, "Judge Condemns 'Mosaic' of Guantánamo Intelligence and Unreliable Witnesses," *Common Dreams*, May 14, 2009, http://www.commondreams.org/headline/2009/05/14-6

**Multilevel Mode**

INFOSEC (information systems security) mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts: a. some users do not have a valid security clearance for all the information processed in the IS; b. all users have the proper security clearance and appropriate formal access approval for that information to which they have access; and c. all users have a valid need-to-know only for information to which they have access.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Multinational Joint Psychological Operations Task Force**

***See Psychological Operations***

A task force composed of PSYOP units from one or more foreign countries formed to carry out a specific PSYOP mission or prosecute PSYOP in support of a theater campaign or other operation. The multinational joint POTF may have conventional non-PSYOP units assigned or attached to support the conduct of specific missions

Source: DoD. *Psychological Operations,* FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

**Multiple Sources**

Two or more source documents, classification guides, or a combination of both.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

---

**~ N ~**

**Named Area of Interest**

The geographical area where information that will satisfy a specific information requirement can be collected. Named areas of interest are usually selected to capture indications of adversary courses of action, but also may be related to conditions of the battlespace.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**National Applications Office**

1. The executive agent to facilitate the use of intelligence community technological assets for civil, homeland security and law enforcement purposes within the United States. The office will begin initial operation by fall 2007 and will build on the long-standing work of the Civil Applications Committee, which was created in 1974 to facilitate the use of the capabilities of the intelligence community for civil, non-defense uses in the United States

Source: DHS, NAO Factsheet, http://www.dhs.gov/xnews/releases/pr_1187188414685.shtm, NAO Charter, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB229/48.pdf , Tim Shorrock, "Bush Goes

Private to Spy on You" CorpWatch November 27, 2007, http://www.truthout.org/docs_2006/120607M.shtml

2. To provide the Department of Homeland Security and civil, state and local emergency planners with imagery and data from satellites run by the National Reconnaissance Office and the National Geospatial Intelligence Agency.

Source: ABC News, http://abcnews.go.com/TheLaw/Story?id=3567635&page=2

**National Asset Database**

***See Critical Infrastructure Information***

1. The USA PATRIOT Act of 2001(P.L. 107-56) defines "critical infrastructure" as: systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Sec. 1016e). This definition was adopted, by reference, by the Homeland Security Act of 2002 (P.L. 107-296, Sec. 2.4) establishing the Department of Homeland Security (DHS). The *National Strategy* also adopts the definition of "critical infrastructure" in P.L. 107-56, and provides the following list of specific infrastructure sectors (and assets) falling under that definition:

Information technology | Telecommunications | Chemicals | Transportation systems | Emergency services | Postal and shipping services| Agriculture and food | Public health and healthcare | Drinking water- water treatment | Energy | Banking and finance | National monuments and icons | Defense industrial base | Key industry-technology sites and Large gathering sites.

For example, out of 33,000 individual assets cataloged in DHS's "national asset database," the agency considers only 1,700, or 5%, to be nationally critical. The 33,000 assets in the DHS database themselves constitute only a subset of all assets in the critical infrastructure sectors

Source: Paul W. Parfomak ."Guarding America: Security Guards and U.S. Critical Infrastructure Protection." November 12, 2004. *CRS Report to Congress* http://www.fas.org/sgp/crs/RL32670.pdf ; John D. Moteff. "Critical Infrastructures: Background, Policy, and Implementation." *CRS Report to Congress* April 18, 2006, http://www.fas.org/sgp/crs/homesec/RL30153.pdf and John Moteff. "Critical Infrastructure: the National Asset Database." *CRS Report to Congres*s September 14, 2006, http://www.fas.org/sgp/crs/homesec/RL33648.pdf.

2. Homeland Security Department has stepped up assurances that it will maintain the confidentiality of critical infrastructure information submitted to the National Asset Database, according to the newly revised draft National Infrastructure Protection Plan Base Plan version

2.0. DHS will evaluate all requests to view the database and will grant access only to select DHS employees and others on a "tightly controlled, need-to-know" basis, the revised plan states.

Source: Alice Lipowicz. "DHS vows to protect info on national database." *Washington Technology* January 24, 2006, http://marc.info/?l=isn&m=113817222815165&w=2

3. The Office of Infrastructure Protection (OIP) in the Department of Homeland Security (DHS) has been developing and maintaining a National Asset Database. The Database contains information on over 77,000 individual assets, ranging from dams, hazardous materials sites, and nuclear power plants to local festivals, petting zoos, and sporting good stores.

Source: John Moteff, "Critical Infrastructure: The National Asset Database," CRS Report to Congress, Updated July 16, 2007, http://www.fas.org/sgp/crs/homesec/RL33648.pdf

**National Cargo Tracking Plan Cargo Tracking**

***See Data Mining***

Department of the Navy. Is used to conduct predictive analysis for counterterrorism, small weapons of mass destruction proliferation, narcotics, alien smuggling, and other high- interest activities involving container shipping activity;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: No;
Features: Private sector data: Yes;
Features: Other agency data: No.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**National Censorship**

***See Censorship***

The examination and control under civil authority of communications entering, leaving, or transiting the borders of the United States, its territories, or its possessions.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**National Clandestine Service (NCS)**

***See HUMINT Manager, Intelligence Information***

Within the CIA to coordinate U.S. HUMINT (human intelligence) efforts; intended to make the

CIA Director "national HUMINT manager" for all fifteen intelligence agencies. to improve cooperation among the spy agencies, as well as streamline the flow of information to elected officials. The 9/11 Commission ("Kean Commission") also recommended

The CIA Director should emphasize (a) rebuilding the CIA's analytic capabilities; (b) transforming the clandestine service by building its human intelligence capabilities; (c) developing a stronger language program, with high standards and sufficient financial incentives; (d) renewing emphasis on recruiting diversity among operations officers so they can blend more easily in foreign cities; (e) ensuring a seamless relationship between human source collection and signals collection at the operational level; and (f) stressing a better balance between unilateral and liaison operations.

The NCS will serve as the national authority for coordination, deconfliction, and evaluation of clandestine HUMINT operations across the Intelligence Community, both abroad and inside the United States, consistent with existing laws, executive orders, and interagency agreements.

Source: National Commission on Terrorist Attacks Upon the United States. Chapter 13. http://www.9-11commission.gov/report/911Report_Ch13.htm ; Joint Inquiry Staff Statement Proposals for Reform within the Intelligence Community. October 3, 2002, http://www.fas.org/irp/congress/2002_hr/100302hill.html; John B. Roberts II. Op-Ed. "Chinese Mole Hunt at CIA." *Washington Times* http://www.mail-archive.com/osint@yahoogroups.com/msg15651.html ; DNI press release "Establishment of the National Clandestine Service (NCS)," October 13, 2005, http://www.dni.gov/press_releases/20051013_release.htm, and Central Intelligence Agency Fact Sheet "Creation of the National HUMINT Manager." October 13, 2005, http://www.fas.org/irp/news/2005/10/dcia101305fs.html

**National Counterterrorism Center**

***See Homeland Security Data Network, Fusion Centers***

Through HSDN, fusion center staff can access the National Counterterrorism Center (NCTC), a classified portal of the most current terrorism-related information

Source: DHS, http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm, ISE, *Annual Report to Congress on the Information Sharing Environment* 2008, http://www.fas.org/irp/agency/ise/2008report.pdf, and http://www.nctc.gov/

**National Crime Information Center (NCIC)**

A nationwide information system dedicated to serving and supporting criminal justice agencies -- local, state, and federal -- in their mission to uphold the law and protect the public. NCIC

2000 serves criminal justice agencies in all 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, and Canada, as well as federal agencies with law enforcement missions. NCIC 2000 provides a major upgrade to those services provided by NCIC [National Crime Information Center], and extends these services down to the patrol car and mobile officer.

NCIC 2000's additional capabilities include **Enhanced Name Search:** Uses the New York State Identification and Intelligence System (NYSIIS); **Fingerprint Searches:** Stores and searches the right index fingerprint. Search inquiries compare the print to all fingerprint data on file (wanted persons and missing persons);**Probation/Parole:** Convicted Persons or Supervised Release File contains records of subjects under supervised release; **Information Linking:** Connects two or more records so that an inquiry on one retrieves the other record(s); **Mugshots:** One mugshot per person record may be entered in NCIC 2000; **Convicted Sex Offender Registry:** Contains records of individuals who are convicted sexual offenders or violent sexual predators; **SENTRY File:** An index of individuals incarcerated in the federal prison system; **Delayed Inquiry:** Every record entered or modified is checked against the inquiry log. Provides the entering and inquiring agency with a response if any other agency inquired on the subject in the last five days, and **On-line Ad-hoc Inquiry**: A flexible technique that allows users to search the active databases and access the system's historical data.

Source: Federal Bureau of Investigation. Criminal Justice Information System. FBI National Crime Information Center, http://www.fbi.gov/hq/cjisd/ncic.htm

**National Declassification Initiative**

This program was conceived in response to an April 2006 audit report by the Information Security Oversight Office (ISOO) entitled "Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes."

Source: NARA, press release, September 6, 2007, http://www.archives.gov/press/press-releases/2006/nr06-137.html

**National DNA Index System (DNS)**

National DNA Index System (NDIS) is a system of DNA profile records input by criminal justice agencies (including state and local law enforcement agencies). The Combined DNA Index System (CODIS) is the automated DNA information processing and telecommunication system that supports NDIS. Pursuant to the DNA Identification Act of 1994 (DNA Act), certain categories of information must be collected: 1) DNA identification records of persons convicted of crimes; 2) Analyses of DNA samples recovered from crime scenes; 3) Analyses of DNA samples recovered from unidentified human remains; 4) Analyses of DNA samples voluntarily contributed from relatives of missing persons; and 5) known reference sample from missing

persons. At state and local levels, in addition to the above specimen categories, state law determines what categories of specimens and what offenses may be included in the database. NDIS does not retain information that would allow the NDIS Custodian to personally identify the record by name or other personal identifier. Individuals seeking to review their records are directed to contact the Federal, State, or local authority that received the DNA sample to obtain instructions on how to access their records. DNA profiles are stored electronically and searched for possible matches.

Source: Department of Justice/Federal Bureau of Investigation, FBI PIA, February 24, 2004, http://foia.fbi.gov/ndispia.htm and CODIS, FBI, http://www.fbi.gov/hq/lab/codis/national.htm

**National Foreign Intelligence Board (NFIB)**

***See National Intelligence Board, United States Intelligence Board***

NFIB will serve as the senior Intelligence Community advisory instrumentality to the Director of Central Intelligence (DC) on the substantive aspects of national intelligence. NFIB will advise the DCI on:

> a. Production, review, and coordination of national foreign intelligence; b. Interagency exchanges of foreign intelligence information; c. Sharing of Community intelligence products with foreign governments; d. Protection of intelligence sources and methods; e. Activities of common concern; f. Such other matters as may be referred to it by the DCI.

Source: Director of Central Intelligence Directive 3/1. January 14, 1997, http://www.fas.org/irp/offdocs/dcid3-1.html

**National Foreign Intelligence Program (NFIP)**

***See National Intelligence Program***

The [former] term "National Foreign Intelligence Program" refers to all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of Central Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

Source: 50 U.S.C. 401a (6)) http://www.law.cornell.edu/uscode/ and Executive Order 12333, http://www.archives.gov/federal-register/executive-orders/1981-reagan.html

**National Ground Intelligence Center**

Premier intelligence analysis organization in DoD...

Providing continuous intelligence on foreign ground forces for the warfighter and supporting decisionmakers...

...From analytic products that ensure U.S. forces and their allies will always have a decisive edge in equipment, organization, and training on any future battlefield...
...To on-the-spot intelligence for the fight...
...To providing information that affects policy decisions at all levels.

In an organizational environment of trust, respect, and communications dedicated to selfless service for the nation.

Source: U.S. Army [See the Wayback Machine, http://web.archive.org/web/20061001024440/http://avenue.org/ngic/Vision.html ]

**National Historical Publications and Records Commission**
A statutory body affiliated with the National Archives and Records Administration (NARA), supports a wide range of activities to preserve, publish, and encourage the use of documentary sources, created in every medium ranging from quill pen to computer, relating to the history of the United States.

Source: NARA, "About NHPRC," http://www.archives.gov/nhprc/about/

**National Industrial Security Program (NISP)**
Established by Executive Order 12829, January 6 1993, "National Industrial Security Program" for the protection of information classified pursuant to Executive Order 12958, April 17, 1995, "Classified National Security Information," or its successor or predecessor orders, and the Atomic Energy Act of 1954, as amended.

The National Security Council is responsible for providing policy direction for the NISP. The Secretary of Defense has been designated Executive Agent for the NISP by the President. The Director, Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP and for issuing implementing binding agency directives. The NISP Operating Manual outlines guidance for facility clearances, classification and marking. Among the goals of NISP are: Achieving uniformity in security procedures; (2) implementing the reciprocity principle in security procedures, particularly with regard to facility and personnel clearances; (3) eliminating duplicative or unnecessary requirements; and (4) achieving reductions in security costs

Source: DoD. National Industrial Security Program Operating Manual (NISPOM). DoD 5220.22-M. Chapter 9. January 1995. http://www.fas.org/sgp/library/nispom/chap_09.htm and ISOO. Report on the

Implementation of the National Industrial Security Program. July 31, 1997, http://www.fas.org/sgp/isoo/nisprept.html

**National Industrial Security Program Operating** Manual (NISPOM; DoD 5220.22-M)

1. Joint Department of Defense, Department of Energy, U.S. Nuclear Regulatory Commission and Central Intelligence Agency industrial and personnel security regulatory manual; NISPOM replaces Department of Defense *Industrial Security Manual for Safeguarding Classified Information*, January 1991. NISPOM defines access, classification and marking rules for contractors.

Source: *National Industrial Security Program Operating Manual* (NISPOM). http://www.fas.org/sgp/library/nispom/foreword.htm and https://www.dss.mil/GW/ShowBinary/DSS/isp/fac_clear/download_nispom.html

2. The Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), is publishing this Directive as a proposed rule and pursuant to section 102(b) (1) of Executive Order 12829, as amended, relating to the National Industrial Security Program. This order establishes a National Industrial Security Program (NISP) to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Redundant, overlapping, or unnecessary requirements impede those interests. Therefore, the NISP serves as the single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests. This Directive sets forth guidance to agencies to set uniform standards throughout the NISP that promote these objectives.

Source: ISOO. "National Industrial Security Program Directive No.1." 32 CFR Part 2004 (Fed Register January 27, 2006), http://www.gpoaccess.gov/fr/index.html

**National Information Infrastructure (NII)**

***See Defense Information Infrastructure, Global information Infrastructure, Information***

1. Nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amount of information available to users. It includes both public and private networks, the Internet, the public switched network, and cable, wireless, and satellite communications.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

2. The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The

national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**National Intelligence**

National intelligence' and `intelligence related to the national security'--
(A) each refer to intelligence which pertains to the interests of more than one department or agency of the Government; and (B) do not refer to counterintelligence or law enforcement activities conducted by the Federal Bureau of Investigation except to the extent provided for in procedures agreed to by the National Intelligence Director and the Attorney General, or otherwise as expressly provided for in this title.

Source: National Intelligence Reform Act of 2004,
http://thomas.loc.gov/cgi-bin/query/F?c108:1:./temp/~c108YGu9x6:e8145:

**National Intelligence Board**

***See National Foreign Intelligence Board***

Advises the DNI on: production, review, and coordination of national intelligence; interagency exchanges of national intelligence information; sharing of IC intelligence products with foreign governments; protection of intelligence sources and methods; activities of common concern and other matters as may be referred to it by the DNI.

Source: ICD 202, http://www.fas.org/irp/dni/icd/icd-202.pdf and
http://www.fas.org/blog/secrecy/2007/08/dni_issues_directives_on_analy.html

**National Intelligence Council**

Established within the Office of the Director of Central Intelligence; composed of senior analysts within the intelligence community and substantive experts from the public and private sector, who shall be appointed by, report to, and serve at the pleasure of, the Director of Central Intelligence. The Council shall—

> (A) produce national intelligence estimates for the Government, including, whenever the Council considers appropriate, alternative views held by elements of the intelligence community;

(B) evaluate community-wide collection and production of intelligence by the intelligence community and the requirements and resources of such collection and production; and

Source: War and National Defense. 50 U.S.C. 15 Subchapter I § 403-3, http://www.gpoaccess.gov/uscode/browse.html

**National Intelligence Program**

***See National Foreign Intelligence Program***

1. There is no perfectly clear line between `national' intelligence and intelligence that supports joint military operations or otherwise supports military requirements. Some `national' systems provide essential support to the military, and some military systems provide intelligence for national needs. The military is the largest consumer and producer of intelligence, and it has needs for intelligence on a 24-hour basis to support military operations around the world. The challenge in reforming the Intelligence Community is to ensure that the needs of national customers and military customers are both met adequately. This bill consolidates the bulk of the intelligence assets under the National Intelligence Director in a way that may make it difficult to ensure adequate intelligence support to the military. As the CSIS 11 stated, `Any successful intelligence reform must respect the military's need to maintain a robust organic tactical intelligence capability and to have rapid access to national intelligence assets and information.'

The bill reported by the Committee contains a definition of the National Intelligence Program (NIP) that may not meet this test, and thus may have harmful unintended consequences. The underlying draft bill said that any program, project or activity of the military departments (namely, the Army, Navy, Air Force and Marines) to acquire intelligence `solely' for the planning and conduct of `tactical' military operations were not part of the NIP.

Source: Carl Levin. Senate Report 108-359 - National Intelligence Reform Act of 2004. to accompany S. 2840 together with Additional Views, http://thomas.loc.gov/cgi-bin/cpquery/T?&report=sr359&dbname=108&

2. The bill [National Intelligence Reform Act of 2004] significantly changes the definition of the National Foreign Intelligence Program. The NIP is defined to include all programs, projects, and activities (whether or not pertaining to national intelligence) of the National Intelligence Authority, the Central Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the Office of Intelligence of the Federal Bureau of Investigation, and the Office of Information Analysis of the Department of Homeland Security. The NIP also includes all national intelligence programs,

projects and activities of the elements of the intelligence community and any other program, project, or activity of a department, agency or element of the United States Government relating to national intelligence unless the NID and the head of the affected entity determine otherwise. These provisions ensure that the NID will have complete budgetary control over the core elements of the intelligence community which produce national intelligence.

The NIP definition specifically excludes programs, projects and activities of the military departments that acquire intelligence principally for the planning and conduct of joint or tactical military operations by the United States Armed Forces. Any assets that are currently in the JMIP but are national and do not acquire intelligence principally for the planning and conduct of joint or tactical military operations by the United States Armed Forces should be moved to the NIP. The inclusion of the word `principally' is meant to reflect that some military assets serve both national and tactical or joint purposes; the mere fact that a DoD asset produces some national intelligence thus does not require that asset to be moved to the NIP.

Source: Senate Report 108-359 - National Intelligence Reform Act of 2004. to accompany S. 2840 together with additional views, http://thomas.loc.gov/cgi-bin/cpquery/T?&report=sr359&dbname=108&

3. NIP encompasses more than half of overall intelligence spending and includes most efforts of the Intelligence Community (IC) -- the CIA, the Defense Intelligence Agency (DIA), the National Reconnaissance Office (NRO), the National Geospatial- Intelligence Agency (NGA) [formerly the National Imagery and Mapping Agency (NIMA)], and the National Security Agency (NSA). In accordance with the Intelligence Reform Act, the DNI has overall responsibility for preparing NIP budget submissions based on priorities established by the President and taking into account input from DOD agencies that have NIP responsibilities. NIP budget totals are authorized in annual intelligence authorization acts; total amounts are specified in the classified schedule that accompany appropriations legislation, but are not made public.

Source: Richard A. Best, Jr. "Intelligence, Surveillance, and Reconnaissance (ISR) Programs: Issues for Congress." *CRS Report to Congress* February 22, 2005, http://www.fas.org/sgp/crs/intel/RL32508.pdf

**National Intelligence Reserve Corps**

The Director of National Intelligence may provide for the establishment and training of a National Intelligence Reserve Corps (in this section referred to as "National Intelligence Reserve Corps") for the temporary reemployment on a voluntary basis of former employees of elements of the intelligence community during periods of emergency, as determined by the Director.

Source: U.S. Code TITLE 50 > CHAPTER 15 > SUBCHAPTER I > § 403-1c
http://www.law.cornell.edu/uscode/50/usc_sec_50_00000403----001c.html

**National Interests**

1. In a very generic sense, national interests are "that which is deemed by a particular state (actor) to be a . . . desirable goal."

Source: G. R. Berridge and Alan James, *A Dictionary of Diplomacy*, Hampshire, UK: Palgrave-Macmillan, Second Edition, 2003, p. 181., cited in Alan G. Stolberg, "Crafting National Interests in the 21st Century, " Ed. J. Boone Bartholomees, Jr., *National Security Policy and Strategy, Guide to National Security Issues* vol. 2 , 3rd ed., U.S. Army War College, 2008. 3-14.
http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB871.pdf

2. The national interest, on the other hand, refers to the well-being of American citizens and American enterprise involved in international relations and afiected by political forces beyond the administrative control of the United States government. (p.6)

it is useful to think of the public interest as being the concern of federal, state, and local government-with the president sharing his authority with Congress, the courts, and the fifty states - and the national interest being the concern only of the federal government, with the President, rather than congress or the courts, exercising the principal authority and responsibility for the nation's welfare. (p.7)

Source: Neuchterlein, Donald E. *United States National Interests in a Changing World*, Lexington: University Press of Kentucky, 1973. 6-7.

**National Media Exploitation Center**

"will serve to advance the IC's collective DOMEX [document and media exploitation] capabilities on behalf of the DNI."

b. DOMEX will support a wide range of intelligence activities…DOMEX reporting and analysis are considered intelligence products. (p.2)

Source: "Document and Media Exploitation" ICD 302, July 6, 2007, http://www.fas.org/irp/dni/icd/icd-302.pdf

**National Operations Security Program**

Created by Reagan National Security Decision Directive (NSDD) 298, January 22, 1988.Each Executive department and agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal Operations Security Program (OPSEC) program with the following common features:

- Specific assignment of responsibility for OPSEC direction and implementation.

- Specific requirements to plan for and implement OPSEC in anticipation of and, where appropriate, during department or agency activity.
- Direction to use OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures.
- Enactment of measures to ensure that all personnel commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process.
- Annual review and evaluation of OPSEC procedures so as to assist the improvement of OPSEC programs.
- Provision for interagency support and cooperation with respect to OPSEC programs.

Agencies with minimal activities that could affect national security need not establish a formal OPSEC program; however, they must cooperate with other departments and agencies to minimize damage to national security when OPSEC problems arise.

Source: FAS. NSDD - National Security Decision Directives, Reagan Administration, http://www.fas.org/irp/offdocs/nsdd298.htm

**National Security**

***See the Gospel of National Security, National Security Information, National Security State***

1. (y) National defense or foreign relations of the United States.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

2. The territorial integrity, sovereignty, and international freedom of action of the United States. Intelligence activities relating to national security encompass all the military, economic, political, scientific, technological, and other aspects of foreign developments that pose actual or potential threats to US national interests.

Source: Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C.: Springfield, VA: National Technical Information Service, [1999?].PREX 3.2: C 76 PREX 3.2/2: G 94

3. Citing Gregory McLauchlan, Hooks (p. 366) writes; "the shift from defense to national security blurred the difference between times of peace and war and put pressure on the U.S. to manage society more intensively at all times."

Source: Gregory Hooks, "The Rise of the Pentagon and U.S. State Building: The Defense Program as Industrial Policy," *The American Journal of Sociology* 96 no.2 (1990):358-404.

4. The definitions of "national security" and what constitutes "intelligence"— and thus what must be classified — are unclear. Boundaries between foreign and domestic information, as well as intelligence and law enforcement, are blurred. (p.11)

Source: Office of the Director of National Intelligence Associate Director of National Intelligence and Chief Information Officer, *Intelligence Community Classification Guidance Findings and Recommendations Report,* January 2008, http://www.fas.org/sgp/othergov/intel/class.pdf

5. (41.) To support the necessarily heavy burdens for national security, the morale of the citizens of the United States must be based both on responsibility and freedom for the individual. The dangers from Soviet subversion and espionage require strong and effective security measures. Eternal vigilance, however, is needed in their exercise to prevent the intimidation of free criticism. It is essential that necessary measures of protection should not be used as to destroy the national unity based on freedom, not on fear.

Source: NSC 162/2 "A Report to the National Security Policy: Basic National Security Policy," October 30, 1953.

6. Security points to some degree of protection of values previously acquired. In Walter Lippmann's words, a nation is secure to the extent to which it is not in danger of having to sacrifice core values, if it wishes to avoid war, and is able, if challenged, to maintain them by victory in such a war. This definition implies that security rises and falls with the ability of a nation to deter an attack, or to defeat it. This is in accord with common usage of the term. (p.147)

In the first place, every increment of security must be paid for by additional sacrifices of other values usually of a kind more exacting than the mere expenditure of precious time on the part of policy makers. (p.158)

Source: Arnold Wolfers. (1962). "National security as an ambiguous symbol." *Discord and Collaboration: Essays on International Politics* Baltimore: Johns Hopkins Press. 148-165.

7. National security is not a value in itself, but rather a condition that allows a nation to maintain its values.

Source: Thomas S. Blanton (2003), "Beyond the Balancing Test: National Security and Open Government in the United States," Ed. Susan L. Maret & Jan Goldman, *Government Secrecy: Classic and Contemporary Readings*. Westport, CT: Libraries Unlimited/Greenwood Press, 2008. 600-626.

8. Note that terms like *national security system*, *national security bureaucracy, national security interests* and *national security policy* are liberally sprinkled throughout the Project on National Security Reform, *Preliminary Findings,* http://www.pnsr.org/data/images/pnsr%20preliminary%20findings%20july%202008.pdf but not defined.

For an historical overview of the evolution of the concept of national security, see Douglas T. Stuart's *Creating the National Security State: A History of the Law that Transformed America* (Princeton University Press, 2008).

**National Security Area (NSA)**
An area established on non-Federal lands located within the United States, its possessions, or territories, for safeguarding classified and/or restricted data information, or protecting DOE (Department of Energy) equipment and/or material. Establishment of an NSA temporarily places such non-Federal lands under the control of the DOE and results only from an emergency event.

Source: DoD. Directive 5100.52, "DoD Response to an Accident or Significant incident involving Radioactive Materials." December 21, 1989, http://www.fas.org/nuke/guide/usa/doctrine/dod/5100-52m/chap2.pdf (replaced by DoD Directive 3150.8, "DoD Response to Radiological Accidents", 06/13/1996)

**National Security Branch**
The National Security Branch (NSB) consists of the FBI's Counterterrorism Division (CTD), Counterintelligence Division (CD), Directorate of Intelligence (DI), and the new Weapons of Mass Destruction Directorate (WMDD) and combines the missions, capabilities, and resources of each. The NSB oversees the national security operations of these four components and is also accountable for the national security functions carried out by other FBI divisions.

(The NSB was established by authority of a June 28, 2005, memorandum from the President directing the Attorney General to implement the WMD Commission's recommendation for the FBI to establish a "National Security Service."

NOTE: the WMD report is here: http://www.gpoaccess.gov/wmd/index.htmlreport/wmd_report.pdf. Try to find a recommendation of this exact entity, "national security service").

Source: FBI, National Security Branch, http://www.fbi.gov/hq/nsb/nsb_faq.htm#established

**National Security Council**

1. The National Security Council (NSC) was established by the National Security Act of 1947 to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. The NSC is the highest Executive Branch entity providing review of, guidance for, and direction to the conduct of all national foreign intelligence and counterintelligence activities. The statutory members of the NSC are the President, the Vice President, the Secretary of State, and the Secretary of Defense. The Director of National Intelligence and the Chairman of the Joint Chiefs of Staff participate as advisors (p.586).

Source: Central Intelligence Agency. "Executive Oversight of Intelligence." *Factbook on Intelligence,* [See the Wayback Machine, http://web.archive.org/web/20060616234124/http://cia.gov/cia/publications/facttell/executive_oversight.html ] and *Congressional Record* January 29, 1952,

2. The NSC lies at the heart of the national security apparatus, being the highest coordinative and advisory body within the Government in this area aside from the President's Cabinet. The Cabinet has no statutory role, but the NSC does. (p.1)

Source: Richard A. Best Jr., "The National Security Council: An Organizational Assessment," *CRS Report to Congress* June 8, 2009, RL30840 http:// www.fas.org/sgp/crs/natsec/RL30840.pdf

**National Security Decision Directive**

***See Presidential Directive***

Issued by the Reagan administration to in creating official national security policy "for the guidance of the defense, intelligence, and foreign policy establishments of the United States government."

Source: Federation of American Scientists. "NSDD – National Security Decision Directives Reagan Administration." http://www.fas.org/irp/offdocs/nsdd/index.html

**National Security Information (NSI)**

***See: Classification Levels, Classified at Birth and Classified Military Information (CMI)***

1. Consists of data, nuclear and otherwise, classified under the authority of various presidential executive orders; this category, according to DeVolpi et al (11-12, 287), is a category of Restricted Data as expressed in the Atomic Energy Act of 1954, and subject to special controls. "Boundless in scope," NSI originated with Carter EO 12065, which DeVolpi and his colleagues (131, 138) refer to as the "National Security Information Executive Order." In 1993, Quist claimed that current authority for classifying information as NSI comes from Executive Order (EO) 12356.

Depending on the degree of harm that unauthorized disclosure could "reasonably be expected to cause"," NSI can be classified as Top Secret, Secret or Confidential (DeVolpi, et al 138).

Source: Alexander DeVolpi et al. *Born Secret: the H-bomb, the Progressive Case and National Security.* New York: Pergamon Press, 1981.

2. National Security Information (NSI) means information that has been determined pursuant to Executive Order 12958 or prior Executive Orders to require protection against unauthorized disclosure and is marked to indicate its classification status when in document form. NSI is referred to as "defense information" in the Atomic Energy Act.

Source: Energy. 10 CFR 1045, http://www.gpoaccess.gov/CFR/index.html

By extension, Bush Executive Order 13292 (March 28, 2003) further expands NSI to information related to

> Military plans, weapons systems, or operations;
> Foreign government information;
> Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
> Foreign relations or foreign activities of the United States, including confidential sources;
> Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
> United States Government programs for safeguarding nuclear materials or facilities;
> Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
> Weapons of mass destruction.

Source: FAS, Executive Order 12065, http://www.fas.org/irp/offdocs/eo/eo-12065.htm; http://www.archives.gov/federal-register/executive-orders/1978.html; Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information," http://www.archives.gov/federal-register/executive-orders/2003.html ; Arvin S. Quist. "Security Classification of Information," http://www.fas.org/sgp/library/quist2/chap_3.html, and Louis Fisher, *Congressional Access to National Security Information* Law Library of Congress May 2009, http://loc.gov/law/help/usconlaw/pdf/GW.2009.pdf

3. Any information that has been determined pursuant to Executive Order 12356 [Clinton; 1995], Executive Order 13292 ["Further Amendment to Executive Order 12958, as

Amended, Classified National Security Information," Bush 2003] or any predecessor order to require protection against unauthorized disclosure and that is so designated. The levels TOP SECRET, SECRET and CONFIDENTIAL are used to designate such information.

Source: DOE Directive. DOE-5631.2c. http://www.fas.org/irp/DoDdir/doe/o5631_2c/o5631_2ca2.htm,

4. Official information or material which requires protection against unauthorized disclosure in the interest of national defense or foreign relations of the United States. The current authority for classifying information as NSI comes from Executive Order (EO) 12356. A declaration of NSI requires prior approval from an authorized person.

Source: DOE. *Understanding Classification*. Washington, D.C.: U.S. Dept. of Energy, Assistant Secretary for Defense Programs, Office of Classification, 1987. SUDOC: E 1.15:0007/1

5. NSI embodies both policy intelligence and military intelligence.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404

**National Security Letters**

1. A type of administrative subpoena which may be issued independently by FBI field offices and not subject to judicial review unless a case comes to court. Under Section 505 of the Patriot Act which authorized FBI field agents to issue national security letters to obtain financial, bank and credit records of individuals.

In certain instances, under 18 U.S.C. 2709, it is possible for the FBI to require the production of records and information pertaining to wire or electronic communications through a National Security Letter, where the only requirement is for the agent of the FBI to certify that the records and information sought are "relevant to an authorized investigation."

Source: Congressional Research Service. "Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations: Background and Proposed Adjustments." April 15, 2005. http://www.fas.org/sgp/crs/natsec/RL32880.pdf and American Civil Liberties Union (ACLU). "Challenging the Constitutionality of the National Security Letter," http://www.aclu.org/nsl/

2. We found that 60 percent of the investigative files we examined contained one or more violations of FBI internal control policies relating to National Security Letters (p.23). Inaccuracies in the OGC (Office of General Counsel) database are outlined in the Executive Summary.

Source: U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, March 2007, http://www.usdoj.gov/oig/special/s0703b/final.pdf (p. xxiii has a useful graphic on FBI use of NSLs).

3. Judge Victor Marrero, of the U.S. District Court in Manhattan, ruled unconstitutional both the gag on recipients of the orders and their lack of judicial scrutiny. It was his second decision striking down national-security letters. Three years ago, he ruled that the orders violated the First Amendment. But an appeals court asked him to reconsider the decision after the Patriot Act was revised this year.

Source: Andrea Foster, *The Wired Campus* http://chronicle.com/wiredcampus/index.php?id=2358 and ACLU, http://www.aclu.org/safefree/nationalsecurityletters/31580prs20070906.html Updated info at: DOJ, Office of the Inspector General, March 2008 *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*,http://www.usdoj.gov/oig/special/s0803b/final.pdf ; **also see** United States. Congress. House. Committee on the Judiciary. Subcommittee on the Constitution, Civil Rights, and Civil Liberties, *National Security Letters Reform Act of 2007* : hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties of the Committee on the Judiciary, House of Representatives, One Hundred Tenth Congress, second session, on H.R. 3189, April 15, 2008, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_house_hearings&docid=f:41795.pdf, United States. Congress. House. Committee on the Judiciary, *Federal Bureau of Investigation.* Part II: hearing before the Committee on the Judiciary, House of Representatives, One Hundred Tenth Congress, second session, April 23, 2008. Washington: U.S. G.P.O., 2008. http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=110_house_hearings&docid=f:41904.pdf and H. R. 3846, FISA Amendments Act of 2009 "To amend the Foreign Intelligence Surveillance Act of 1978 to provide additional civil liberties protections, and for other purposes," 111th Congress, 1st session, October, 20, 2009, http://thomas.loc.gov/cgi-bin/query/z?c111:H.R.3846:

4. Five federal statutes authorize various intelligence agencies to demand, through National Security Letters (NSLs), certain customer information from communications providers, financial institutions, and consumer credit reporting agencies, under the Right to Financial Privacy Act, the Fair Credit Reporting Act, the National Security Act, and Electronic Communications Privacy Act. The USA PATRIOT Act expanded NSL authority. Later reports of the Department of Justice Inspector General indicated that (1) the FBI considered the expanded authority very useful; (2) after expansion the number of NSLs requests increased dramatically; (3) the number of requests relating to Americans increased substantially; and (4) FBI use of NSL authority had sometimes failed to comply with statutory, Attorney General, or FBI policies.

Originally, the NSL statutes authorized nondisclosure requirements prohibiting recipients from disclosing receipt or the content of the NSL to anyone, ever. They now permit judicial review of

these secrecy provisions. As understood by the courts, recipients may request the issuing agency to seek and justify to the court the continued binding effect of any secrecy requirement.

Source: Charles Doyle, "National Security Letters: Proposed Amendments in the 111th Congress," *CRS Report to Congress* October 28, 2009, R40887, http://opencrs.com/document/R40887/

5. The ancestor of the first NSL letter provision is a statutory exception to privacy protections afforded by the Right to Financial Privacy Act (RFPA).11 Its history is not particularly instructive and consists primarily of a determination that the exception in its original form should not be too broadly construed.12 But the exception was just that, an exception. It was neither an affirmative grant of authority to request information nor a command to financial institutions to provided information when asked. It removed the restrictions on the release of customer information imposed on financial institutions by the Right to Financial Privacy Act, but it left them free to decline to comply when asked to do so.

Source: Source: Charles Doyle, "National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments," *CRS Report to Congress* September 8, 2009, RS22406 http://www.fas.org/sgp/crs/intel/RS22406.pdf

**National Security Presidential Directive (NSPD)**

***See Presidential Directive***

In the George W. Bush Administration, the directives that are used to promulgate Presidential decisions on national security matters are designated National Security Presidential Directives.

As discussed in NSPD 1, this new category of directives replaces both the Presidential Decision Directives and the Presidential Review Directives of the previous Administration. Unless other otherwise indicated, however, past Directives remain in effect until they are superseded. On October 29, 2001, President Bush issued the first of a new series of Homeland Security Presidential Directives (HSPDs) governing homeland security policy.

Source: Federation of American Scientists. "National Security Presidential Directive: George W. Bush Administration." http://www.fas.org/irp/offdocs/nspd/index.html

**National Security Sensitivity Levels**

Federal employment positions as defined by the US Office of Personal Management. Special-Sensitive (SS)

- Includes any positions that the head of the agency determines to be in a level higher than Critical-Sensitive because of special requirements under authority other than EO

10450 and EO 12968 (e.g., D.C.ID 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)).

Critical-Sensitive (CS) Potential for exceptionally grave damage to the national security; Includes positions involving any of the following:

- Access to Top Secret national security information or materials;
- Requirement for a Department of Energy (DOE) "Q" security clearance for access to DOE national security information, materials, and/or sites.
- Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.
- Investigative duties, the issuance of personnel security clearances, or duty on personnel security boards.
- Commissioned law enforcement duties.

  Other positions related to national security, regardless of duties, that require the same degree of trust.

Noncritical-Sensitive (NCS) Potential for damage to serious damage to the national security: Includes positions involving any of the following:

- *Access to Secret or Confidential national security information or materials;
- *Requirement to obtain a Department of Energy (DOE) "L" security clearance for access to DOE national security information, materials, and/or sites;
- Duties that may directly or indirectly adversely affect the national security operations of the agency.

Source: Office of Personnel Management. "National Security Positions." 5 CFR 732, http://www.gpoaccess.gov/cfr/index.html

**National Security Space Programs**

Third, U.S. national security space programs are vital to peace and stability, and the two officials primarily responsible and accountable for those programs are the Secretary of Defense and the Director of Central Intelligence. Their relationship is critical to the development and deployment of the space capabilities needed to support the President in war, in crisis and also in peace. They must work closely and effectively together, in partnership, both to set and maintain the course for national security space programs and to resolve the differences that arise between their respective bureaucracies. Only if they do so will the armed forces, the Intelligence Community and the National Command Authorities have the information they need

to pursue our deterrence and defense objectives successfully in this complex, changing and still dangerous world.

Source: Report of the Commission to Assess United States National Security Space Management and Organization Pursuant to P.L. 106-65, January 11, 2001, p. 10, http://www.dod.mil/pubs/spaceabout.html

**National Security State**

***See National Security***

1. The American state must act for itself and for the world against those who we deem as enemies. Virtually all of these activities and assumptions are grounded in past identifiable laws, rules, secret regulations, and bureaucratic structures that determine the present and future. In other words, President George W. Bush did not have to start *de novo*.

Republican and Democratic and administrations alike operated a National Security State through countless regulations, secret memoranda, defense contracts, wiretaps, and hardware acquisitions which laid the groundwork for the current Bush administration's response. From FDR forward, American political, economic, and military elites shared in the creation of the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Department of Defense (DoD), the Department of Energy (DOE), the National Reconnaissance Office (NRO), and dozens of other bureaucracies. They collaborated in extending the power and reach of the Federal Bureau of Investigation (FBI). This framework is woven into America's social fabric, including its educational institutions, corporations, scientific enterprises, and the media.

Source: Marcus G. Raskin and A. Carl LeVan."The National Security State and the Tragedy of Empire." In Marcus G. Raskin and A. Carl LeVan. *In Democracy's Shadow: the Secret World of National Security.* New York: Nation Books, 2005. 3-42.

2. Defining characteristics of the national security state:

- Organizing for war, Cold War, and limited war (Raskin & LeVan)
- Control of the public sphere (Raskin & LeVan)
- Limiting or undermining individual rights (Raskin & LeVan)
- Control and protection of information across tiers
- Emphasis on surveillance, with a rise in the technological ability to capture, record, and manipulate information
- Covert actions and the rise of secrecy regarding state actions
- Nuclear weapons are a key component of the NSS (Dwyer & Dwyer 185; e.g., Atomic Energy Act of 1948, 1954); this information must be protected

- Evolution from a war state into a security state
- Federal (and local) law enforcement metamorphosing into security enforcement (Raven-Hansen 217)

Source: Anabel L. Dwyer and David J. Dwyer. "Courts and Universities as Institutions in the National Security State," In Marcus G. Raskin and A. Carl LeVan. *In Democracy's Shadow: the Secret World of National Security.* (New York: Nation Books, 2005. 165-203); Peter Raven-Hansen, "Security's Conquest of Federal Law Enforcement," In Marcus G. Raskin and A. Carl LeVan. *In Democracy's Shadow: the Secret World of National Security* (New York: Nation Books, 2005. 217-236), and Marcus G. Raskin and A. Carl LeVan, "The National Security State and the Tragedy of Empire," In Marcus G. Raskin and A. Carl LeVan. *In Democracy's Shadow: the Secret World of National Security.* (New York: Nation Books, 2005. 3-42).

3. The Eisenhower "national defense standard," extended to "interest of national defense or foreign relations of the United States (collectively termed 'national security').

Source: Arthur Schlesinger, *The Imperial Presidency*. New York: Atlantic Monthly, 1973. 49.

**National Security Strategy**
The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national security. Also called national strategy or grand strategy. (JP 3-0)

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**National Security System**
Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapon system; or 56. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management).

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
and 40 U.S.C. 1452, http://www.gpoaccess.gov/uscode/browse.html

**National Strategy**
The art and science of developing and using the diplomatic, economic, and informational

powers of a nation, together with its armed forces, during peace and war to secure national objectives. Also called national security strategy or grand strategy.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Naval Nuclear Propulsion Information (NNPI)**
NNPI concerns all classified and controlled unclassified information related to the naval nuclear propulsion program. This marking supplements existing classification and control systems and is not a separate category outside of the authorities provided under the AEA or Executive Order 12958 for, as an example, classified NNPI. The use of "NNPI" is an additional marking applied to some of the previously defined categories of information to indicate additional controls for protection or access.

Source: GAO. *Managing Sensitive Information: Actions Needed to Ensure Recent Changes in DOE Oversight Do Not Weaken an Effective Classification System*. June 26, 2006, http://www.gao.gov/new.items/d06785.pdf

**Need-to-Know**

1. Garrett (1) writes that Executive Order 10501 ("Safeguarding Official Information in the Interests of the Defense of the United States, "November 5, 1953) "establishes the basis for the need-to-know concept":

"Knowledge or possession of classified defense information shall be permitted only to persons whose official duties require such access in the interest of promoting national defense and if they have been determined to be trustworthy."

Need-to-know is defined by DoD Directive 5200.1 Subsection VII.D, Enclosure 1 as:

"The dissemination of classified information orally, in writing, or by any other means, shall be limited to those persons whose official duties require knowledge or possession thereof."

Source: C. Donald Garrett. "The Role of 'Need-to-Know' in Releasing Classified Information." *Defense Industry Bulletin* 5 no. 2 (February 1969): 1-3.

2. A determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.

Source: DoD. Defense Personnel Security Research Center. "Employees Guide to Security Responsibilities." http://www.hq.nasa.gov/office/ospp/securityguide/Home.htm

3. A determination by a person having responsibility for classified information or material, that a proposed recipient's access to such classified information or matter is necessary in the performance of official or contractual duties of employment.

Source: DOE. Department of Energy Directive DOE-5631.2c, http://www.fas.org/irp/doddir/doe/o5631_2c/index.html

4. A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of classified information in order to accomplish lawful and authorized Government purposes.

Source: U.S. Department of Justice. United States Marshals Service. Office of Inspections. Internal Security Division. *Information Security*. Washington D.C.: 1991. SUDOC: J 25.2: In 3

5. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

6. A determination by an authorized holder of classified information that access to specific classified material in their possession (typo in NIMA doc here) is required by another person to perform a specific and authorized function to carry out a national task. Such person shall possess an appropriate clearance and access approvals in accordance with D.C.ID 1/14.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

7. In addition to a security clearance, a person must have a need to have access to the particular classified information or material sought in connection with the performance of his/her official duties or by contractual obligations. The determination of that need will be made by the official(s) having responsibility for the classified information or material.

Source: U.S.G.S. "National Security Position Handbook 440-7-H, Glossary of Definitions." March 2004, http://www.usgs.gov/usgs-manual/handbook/hb/440-7-h/440-7-h-appa.html

8. Requested information is pertinent and necessary to the requestor agency in initiating, furthering, or completing an investigation.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404

9. A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

10. "Need-to-know" is the determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Such persons shall possess an appropriate security clearance and access approval granted pursuant to Executive Order 12968, Access to Classified Information.

Source: Director of Central Intelligence "Directive 1/7 Security Controls on the Dissemination of Intelligence Information." 3.6June 30, 1998, http://www.fas.org/irp/offdocs/D.C.id1-7.html

11. Need-to-know demands not merely that customers receive only what they need, but also that they receive all the information they need to carry out their missions. To effectively implement this directive, IC agencies must work cooperatively with customers to understand their requirements and ensure that they receive all applicable intelligence information while minimizing the risk of unauthorized disclosure. Customers, in turn, will be responsible for ensuring the application of need-to-know within their organizations.

Source: Director of Central Intelligence Directive 8/1. "Intelligence Community Policy on Intelligence Sharing." June 4, 2004, http://www.fas.org/irp/offdocs/dcid8-1.html

**Need to Know Determination**

1. Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

2. Need to know means a determination by a person having responsibility for protecting Safeguards Information that a proposed recipient's access to Safeguards Information is necessary in the performance of official, contractual, or licensee duties of employment. [46]

Source: Energy. 10 CFR 73, http://www.gpoaccess.gov/CFR/index.html; Executive Order 10501 (Safeguarding Official Information in the interests of the Defense of the United States), November 5, 1953 establishes the basis for the need-to-know concept.

**Netwar**

***See Cyberwar, Defensive Information Warfare, Direct Information Warfare, Information Warfare, Strategic Information Warfare***

Refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt or damage what a target population knows or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.

Source: John J. Arquilla and David F. Ronfeldt. "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict. " *Rand Research Review* xix no. 2 (1995), http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html

**Next Generation Identification (NGI) System**

***See FBI Center for Biometric Excellence***

The NGI System will advance the integration strategies and indexing of additional, lawfully authorized, biometric data, providing the framework for a future multimodal system which will facilitate biometric fusion identification techniques. This framework will be expandable,

[46] The Nuclear Regulatory Commission changed regulations to expand the categories of people who may seek access to classified information associated with NRC regulated activities to include environmental and public interest organizations. The categories of facilities that may be authorized to store such information will also be expanded. The regulations changed on July 5, 2005. The new regulations will allow potential intervenors to seek access authorizations and facility security clearances. http://www.ens-newswire.com/ens/jun2005/2005-06-02-09.asp

scalable, and flexible to accommodate new technologies and emerging biometrics standards, and will be interoperable with existing biometric systems.

Source: FBI Press Release, "FBI Announces Contract Award for Next Generation Identification System," February 12, 2008, http://www.fbi.gov/pressrel/pressrel08/ngicontract021208.htm and Richard Koman, "FBI planning massive database," *ZDNe*t December 24, 2007, http://government.zdnet.com/?p=3580

**NICKA**

***See Code Word / Codeword, Exercise Term, Nickname***

The Code Word, Nickname and Exercise Term (NICKA) system is designed to fully automate the OSD requirement for maintenance of code words, nicknames, exercise terms, and reconnaissance nicknames data by the Joint Staff. NICKA maintains records of all reported code words and their status, all reconnaissance nicknames used at the Joint Reconnaissance Center, all exercise terms, and all currently authorized nicknames. The system validates code word and nickname usage with assigned agencies and ensures that authorized nicknames and code words are not duplicated. The NICKA transaction provides a way to register and maintain code words, nicknames, and exercise terms. NICKA currently resides in the Global Command and Control System, classified Top Secret (GCCS (TS)).

Source: Chairman of the Joint Chiefs of Staff Manual. *Code Word, Nickname and Exercise Term Report (Short Title – NICKA).* April 1998, http://fas.org/irp/doddir/dod/cjcsm3150_29a.pdf

**Nickname**

***See Code Names, Code word / Codeword, Exercise Term, NICKA***

1. Assignment of the first word nickname identifies the using agency; Nicknames may be assigned to actual, real-world events, projects, movement of forces, and other nonexercise activities involving elements of information of any classification category. However, the nickname with the description or meaning it represents along with the relationship of the nickname and its meaning must be unclassified. A nickname is not designed to achieve a security objective.

Source: HQ North American Aerospace Defense Command NORAD Regulation 11-3. Peterson Air Force Base, Colorado 80914-5002 25, August 1989. "Code Words, Nicknames and Exercise Terms." http://www.fas.org/spp/military/docops/norad/reg11003.htm

2. A combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

3. Nicknames are assigned by NICKA; In 1975, the JCS implemented these guidelines by establishing a computer system to fully automate the maintenance and reconciliation of nicknames, code words, and exercise terms. [76] The computer system, called the Code Word, Nickname, and Exercise Term System (an unwieldy name shortened to NICKA), is still in operation today and can be accessed through the Worldwide Military Command and Control System. The NICKA system is not, as some assume a random word generator for nicknames; it is, in fact, merely an automated means for submitting, validating, and storing them. The authority to create nicknames rests not with those who manage the NICKA system, but with 24 DOD components, agencies, and unified and specified commands.[77] JCS assigns each of these organizations a series of two-letter alphabetic sequences and requires that the first word of each two-word nickname begin with a letter pair from one of the sequences.[78] For example, the US Atlantic Command (USACOM) is assigned six two-letter alphabetic sequences: AG-AL, ES-EZ, JG-JL, QA-QF, SM-SR, and UM-UR.[79] Selecting the letter pair UR from the last of these sequences, a staff officer recommended the nickname Urgent Fury for the 1983 invasion of Grenada.

Source: Gregory C. Sieminski. "The Art of Naming Operations." Parameters: US Army War College Quarterly Autumn 1995, http://carlisle-www.army.mil/usawc/Parameters/1995/sieminsk.htm

4. Nicknames may be assigned to actual, real-world events, projects, movement of forces, or other non-exercise activities. They may involve information of any classification, but the nickname and the description or meaning it represents must be unclassified. A nickname is not designed to achieve a security objective

Source: Department of the Navy, "Code Word, Nicknames, and Exercise Terminology System," OPNAVINST 5511.37D, January 30, 2007. http://www.fas.org/irp/doddir/navy/opnavinst/5511_37d.pdf

## Nondisclosure Agreements

1. A confidentiality agreement; a contract to protect the confidentiality of secret information that is disclosed during employment or another type of business transaction.

Source: National Defense. 32 CFR 2003, http://www.gpoaccess.gov/cfr/index.html; NARA, EO 12958 http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html and Briefing Booklet, http://www.archives.gov/isoo/training/standard-form-312.pdf

2. SF 312, SF 189, and SF 189-A are nondisclosure agreements between the United States and an individual; All employees of executive branch departments, and independent

agencies or offices, who have not previously signed the SF 189, must sign the SF 312 before being granted access to classified information.

Source: Defense Security Service. "Classified Information Nondisclosure Agreement." http://www.dtic.mil/whs/directives/infomgt/forms/eforms/sf0312.pdf and http://www.dss.mil/files/pdf/new_sf312.pdf

3. DHS Form 11000-6, Sensitive But Unclassified Information Nondisclosure Agreement (NDA), as a condition of access to such information. Others not contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager. The revised DHS policy invalidates previously signed NDAs. Pursuant to the revised policy, DHS Office of Security will develop and implement an education and awareness program for the safeguarding of SBU information. Once the program is developed and appropriate notifications are provided, all employees will participate in classroom or computer-based training sessions designed to educate employees on what constitutes SBU information.

Source: Department of Homeland Security Management Directive 11042, http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf; DHS Management Directive 11042.1, revised January 6, 2005, http://www.fas.org/sgp/othergov/dhs20050111.pdf and FAS, *Secrecy News* January 12, 2005, http://www.fas.org/sgp/news/secrecy/2005/01/011205.html

**Nonorganic Intelligence Support**

***See HUMINT, PSYOP***

Organic intelligence support rarely provides all of the necessary information required for PSYOP units to plan, produce, disseminate, and evaluate the PSYOP effort. Therefore, PSYOP S-2s must leverage the available intelligence assets that are external to the PSYOP community. PSYOP depend on HUMINT, signal intelligence (SIGINT), imagery intelligence (IMINT), open-source intelligence (OSINT), technical intelligence (TECHINT), and counterintelligence (CI) support to plan their missions. These intelligence disciplines are discussed in the following paragraphs.

Source: DoD Psychological Operations, FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

**North Atlantic Treaty Organization Information (NATO)**

***See Classification Markings/ Control Markings***

1. Except for the foreign security classification designation RESTRICTED, foreign classification designations, including those of international organizations of governments, e.g., NATO, generally parallel U.S. classification designations. A table of equivalents is contained in 12 FAM 529 Exhibit 529.13-1.

Source: Department of State. *Foreign Service Manual*. 12FAM529.11 "Identification, Marking and Handling." http://www.state.gov/m/a/dir/regs/

2. NATO CLASSIFIED has four levels of classified information:

- COSMIC TOP SECRET (CTS)
- NATO SECRET (NS)
- NATO CONFIDENTIAL (NC)
- NATO RESTRICTED (NR)

The North Atlantic Council of NATO has agreed that each member nation will establish a national security authority responsible for the security of NATO classified information within its country and in its national agencies abroad.

Source: Department of Energy DOE M 471.2-1 "Manual for Classified Matter Protection and Control." September 26, 1995. http://fas.org/irp/doddir/doe/m471_2-1.htm;
DoD Directive 5100.55 "United States Security Authority for North Atlantic Treaty Organization Affairs." April 21, 1982, http://www.dtic.mil/whs/directives/corres/html/510055.htm

**Not in the circle of love**

***See Need to Know***

JEREMY SCAHILL: And this Blackwater program is an outgrowth of that separating of JSOC from the broader military chain of command, and that is why my sources say there are senior figures within the military and the a administration right now that may be unaware of it because as he said, "They are not in the circle of love."

AMY GOODMAN: "Not in the circle of love?"

JEREMY SCAHILL: That is the phrase that was used twice by the military intelligence source that I spoke to. What we are seeing now, and I also talked to Colonel Lawrence Wilkerson, who was the Chief of Staff to then Secretary of State Colin Powell. And he described, he first of all, when I talked about this, said the program would not surprise him, and that he was very disturbed when he sees execute orders the coming out ,saying that JSOC is essentially above the Special Operations Command and the Special Operations Command is essentially in a support role for these JSOC teams. So, what I am told is that this program is so compartmentalized, that there are probably very top-level people that are unaware of it, and in fact, what my military intelligence source says, is that Blackwater personnel that are working as part of this program, and have worked as part of this program, have been given rolling security clearances above their actual security clearance.

Source: Jeremy Scahill, "Blackwater's Secret War in Pakistan: Jeremy Scahill Reveals Private Military Firm Operating in Pakistan Under Covert Assassination and Kidnapping Program," Novermber 24, 2009, Democracy Now http://www.democracynow.org/2009/11/24/blackwaters_secret_war_in_pakistan_jeremy and Scahill, "The secret war in Pakistan," *The Nation* November 23, 2009 http://www.thenation.com/doc/20091207/scahill

**Novel Intelligence from Massive Data (NIMD)**

***See Advanced Research Development Activity (ARDA)***

The Novel Intelligence from Massive Data program is aimed at focusing analytic attention on the most critical information found within massive data – information that indicates the potential for strategic surprise. *Novel Intelligence* is actionable information not previously known to the analyst or policy makers. It gives the analyst new insight into a previously unappreciated or misunderstood threat. *Massive data* has multiple dimensions that may cause difficulty, some of which include volume or depth, heterogeneity or breadth, and complexity.

That is, data may be "massive" because of the sheer quantity of similar items, typically a petabyte or more. Some intelligence data sources grow at the rate of four petabytes per month now, and the rate of growth is increasing. A smaller volume of data may nonetheless be considered "massive" because it consists of separately authored information objects in numerous types and formats: structured text in various formats, unstructured text, spoken text, audio, video, tables, graphs, diagrams, images, maps, equations, chemical formulas, etc. Data may also be deemed "massive" because of its inherent complexity, which arises when a single document contains links between multiple information objects, with the meaning of any object dependent on information contained within other objects. Understanding the content of complex data requires being able to process data that has already been fused together, which is beyond the capability of current technology. A deeper level of complexity comes into play when information requires a variety of expertise for full comprehension because of the interconnectedness of the domains.

Source: Intelligence Community Advanced Research and Development Activity (ARDA). NIMD. [See the Wayback Machine, http://web.archive.org/web/20050610014439/http://ic-arda.org/Novel_Intelligence/index.html ] and Jeffrey W. Seifert. "Data Mining: An Overview." *CRS Report for Congress* January 27, 2006, http://www.fas.org/sgp/crs/secrecy/RS20748.pdf

---

**~ O ~**

**OBSCENE File**

1. Obscene or pornographic materials "that may arouse the curiosity of Bureau employees" that were restricted by the Hoover FBI.

2. March 24, 1925 Bureau Director Hoover authorizes a special OBSCENE letter procedure and creates a separate OBSCENE File for agent reports on "obscene or improper" materials.

Source: Athan Theoharis, ed. *The FBI: A Comprehensive Reference Guide*. Phoenix: Oryx Press, 1998. 363.

**Of Official Concern**
***See Prepublication Review***
Materials are *on matters* of official concern if they relate to any policy, program, or operation of the employee's agency or to current U.S. foreign policies, or reasonably may be expected to affect the foreign relations of the United States.

Source: U.S. Department of State. 3 FAM 4172 1-3(A), http://www.state.gov/m/a/dir/regs/

**Offensive Counterinformation**
Actions against the adversary's information functions.

Source: Department of the Air Force. "Cornerstones of Information Warfare." 1995,
[At the Wayback Machine,
http://web.archive.org/web/20040901091302/http://www.af.mil/lib/corner.html]

**Offensive Information Operations**
1. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical destruction, and special information operations, and could also include computer network attack. (Army) The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decisionmakers or to influence others to achieve or promote specific objectives.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004,
http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents
and Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

### Office of Censorship

Provides for the Secretary of Defense to exercise on interim basis pending operational readiness of the Office of Censorship, censorship of communications crossing the borders of the United States and any of its territories or possessions.

The Director of Censorship is hereby authorized and directed to request and coordinate the voluntary cooperation of the domestic press, radio and television broadcasters and motion picture producers in the withholding from publication military and other information which should not be released in the interest of effective prosecution of war.

Source: Eisenhower Emergency Action Document, "Executive Order to establish the Office of Censorship, and describing its functions and duties," initiated by Office of Defense Mobilization, 1956 crafted to support "Operation Alert"; Dee Garrison, *Bracing for Armageddon: Why Civil Defense Never Worked* New York: Oxford University Press, 2006; and CONELRAD, The Eisenhower 10, http://www.conelrad.com/atomicsecrets/secrets.php?secrets=e18

### Office of Global Communications

The mission of the Office shall be to advise the President, the heads of appropriate offices within the Executive Office of the President, and the heads of executive departments and agencies (agencies) on utilization of the most effective means for the United States Government to ensure consistency in messages that will promote the interests of the for and among coalition partners of the United States, and inform international audiences. The Office shall provide such advice on activities in which the role of the United States Government is apparent or publicly acknowledged.

Source: Executive Order 13283, "Establishing the Office of Global Communications." January 21, 2003, http://www.archives.gov/federal-register/executive-orders/2003.html

### Office of Strategic Influence

*See Information Operations Task Force*

In November 2001, the Office of the Secretary of Defense (OSD) stood up the Office of Strategic Influence under the direct supervision of the Under Secretary of Defense for Policy (USD-P). OSI was designed to provide DoD with a series of information policy options and programs that conducted worldwide and target specific analysis and opinion polls. OSI was also tasked to initiate programs that countered hostile propaganda, misinformation and disinformation directed against the United States and its allies from foreign sources. The organization was composed of civilian and military personnel with interagency, informational, technological and regional expertise and placed under the direction of Brigadier General Simon P. Worden, a highly experienced influence specialist, astro-scientist and technologist from USSPACECOM.

Informed speculation has it that while OSI was highly successful in determining its baseline mission requirement against the GWOT [47] and beginning to execute pro-US influence programs abroad, it was not capable of protecting itself from political "rice bowl" issues and petty jealousies. When a series of coordinated press releases with intentionally leading disinformation hit the media on the February 20, 2002, a media feeding frenzy against OSI ensued. DoD decided to close the office rather than counter the internally spread disinformation and take corrective actions to eliminate leaks and security violations. Since OSI was dissolved, no other organization within the interagency has attempted to identify, coordinate, synchronize and conduct long-term, analytically based, influence programs in support of the U.S. government in the global environment.

Source: Col. Brad M. Ward. *Strategic Influence Operations – The Information Connections.* Army War College. April, 2003, http://www.fas.org/irp/eprint/ward.pdf

**Official DoD Information**

All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department.

Source: DoD, "Clearance of DoD Information for Public Release," DoD Directive 5230.09, August 22, 2008, http://www.fas.org/irp/doddir/dod/d5230_09.pdf

**Official Information**

***See Closed Information, Twilight Information***

Information which is owned by, produced for or by, or is subject to the control of the United States Government. *All classified information is considered official information*. [emphasis added]

Source: DoD. Defense Personnel Security Research Center. "Employees Guide to Security Responsibilities." http://www.hq.nasa.gov/office/ospp/securityguide/Home.htm

**Official Use Only**

1. A designation identifying a certain unclassified but sensitive information that may be exempt from public release under the Freedom of Information Act; or

2. A security classification marking used during the period July 18, 1949 through October 22, 1951.

---

[47] The Global War on Terror appears to have shifted to "Overseas Contingency Operations," see *Washington Post* March 25, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/03/24/AR2009032402818.html

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

3. On April 9, 2003, DOE issued directives that formally established an OUO program within DOE for the first time since the Atomic Energy Commission. These directives apply to all DOE and National Nuclear Security Administration (NNSA) elements that (1) identify information under their cognizance as OUO and mark documents accordingly, or 2. possess documents marked as OUO by other DOE elements or marked with other agency markings equivalent to OUO (e.g., DoD "For Official use Only"; Department of State's "Sensitive But Unclassified.")

*Any employee, federal or contractor can determine that an unclassified document contains OUO information* [emphasis added] if that document is originated within his/her office, or is under the control of his/her office. No special authority or training is required. As outlined in the manual, the first step is for the employee to determine if the information has the potential to damage Governmental, commercial, or private interests if given to someone who doesn't need it to perform his/her job or other DOE authorized activity.

Source: DOE Manual 471.3-1 and DOE Communiqué. vol. 20 no. 1 February 2004, http://www.fas.org/sgp/othergov/doe/comm0204.pdf

**OIG--Project Strikeback**

***See Data Mining***

Department of Education. Compares Department of Education and Federal Bureau of Investigation data for anomalies. Also verifies personal identifiers;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. Data Mining: Federal Efforts Cover a Wide Range of Uses. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Open Source Center**

1. Based at the CIA, the Center will advance the Intelligence Community's exploitation of openly available information to include the Internet, databases, press, radio, television, video, geospatial data, photos and commercial imagery. The Center's functions will include collection, analysis and research, training and information technology management to facilitate government-wide access and use. The Center will build on the established expertise of the

CIA's Foreign Broadcast Information Service (FBIS), which has provided the U.S. Government a broad range of highly valued products and services since 1941. The Director of the CIA will administer the Center on behalf of the DNI.

Source: Office of the Director of National Intelligence. November 8, 2005, http://www.dni.gov/press_releases/20051108_release.htm

2. Based at CIA, effective 1 November 2005. The Center will build on the established expertise of the CIA's Foreign Broadcast Information Service (FBIS) — an organization that enjoys a long history of providing the US government highly valued open source products and services. The Center's functions will include collection, analysis and research, training, and information technology management to facilitate government-wide access and use.

Source: Central Intelligence Agency. Press Release. November 8, 2005. [See the Wayback Machine, http://web.archive.org/web/20060705165235/http://www.cia.gov/cia/public_affairs/press_release/2005/pr11082005.html ]and *Secrecy News* May 18, 2008 "Open Source Center Keeps Public in the Dark," http://www.fas.org/blog/secrecy/2008/05/open_source_cent.html

**Open Source Information**

1. Information that is publicly available (for example, any member of the public could lawfully obtain information by request or observation), as well as other unclassified information that has limited public distribution or access. Open-source information also includes any information that may be used in an unclassified context without compromising national security or intelligence sources or methods. If the information is not publicly available, certain legal requirements relating to collection, retention, and dissemination might apply.

Source: Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence: Gaining Knowledge and Foreknowledge of the World around Us*. Washington, D.C.: Springfield, VA: National Technical Information Service, [1999?]. SUDOC: PREX 3.2: C 76 and PREX 3.2/2: G 94

2. Publicly available information (that is, information that any member of the public could lawfully obtain by request or observation), as well as other unclassified information that has limited public distribution or access (including information from companies, academia and other sources). Access to such information may or may not require payment.

Source: Federal Geographic Data Committee. Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns." June 2005, http://www.fas.org/sgp/othergov/fgD.C.0605.pdf

3. October 1, 2005, the CIA's "open source" unit will be operational, scanning Websites, newspapers, radio, television, [the infocommons in other words].

Source: Timothy J. Burger. "Opening up the CIA." *Time* 166 no. 7 (August 15, 2005).

**Open Source Information System**

Information network which provides access to U.S. Government and other open source collections.

Source: Defense Technical Information Center (DTIC). Public STINET Glossary. http://stinet.dtic.mil/help/acronyms.html and FAS.http://www.fas.org/irp/program/disseminate/osis.htm

**Open-Source Intelligence**

1. Information of potential intelligence value that is available to the general public.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

2. Highly classified messages or analytical products underwent a sanitation process which tended to remove important details. The end result was intelligence reports which were too general or broad to be of much use. An attempt to disseminate highly classified documents down to port of entry level, resulted in the discovery that few if any personnel at that level had the requisite clearances. In other instances, the necessary security infrastructure was unavailable.

…given the largely unclassified nature of open source intelligence products, the aforementioned issues of clearances and security infrastructure are irrelevant. Not only can these OSINT products be disseminated to inspectors at a port of entry, they can also be provided to state and local law enforcement. In fact, OSINT products could be disseminated to the full compliment of first responders such as firefighters, EMT's university police departments, hospitals and full security firms. Consider for a moment what a paradigm shift that would represent.

Source: Eliot A. Jardines, President, Open Source Publishing, Incorporated's (OSP) *and* Assistant Deputy Director of National Intelligence for Open Source. Before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. Hearing on "Using Open-Source Information Effectively." June 21, 2005. 1-2, http://www.osint.org/testimonyjardines.pdf

3. Open source information, according to some observers, generally falls into four categories: widely available data and information; targeted commercial data; individual experts; and "gray" literature, which consists of written information produced by the private sector,

government, and academe that has limited availability, either because few copies are produced, existence of the material is largely unknown, or access to information is constrained. Within these four categories, open source information can include:

- media such as newspaper, magazines, radio, television, and computer-based information;
- public data such as government reports, and official data such as budgets and demographics, hearings, legislative debates, press conferences, and speeches;
- information derived from professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts;
- commercial data such as commercial imagery; and,
- gray literature such as trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, and market surveys.

Open source information also can include information, which although unclassified, could be considered company proprietary, financially sensitive, legally protected, or personally damaging.24 With increasing frequency, it also includes information derived from Internet blogs. According to Intelligence Community officials, blogs are providing "a lot of rich information that are telling us a lot about social perspective and everything from what the general feeling is[,], to ... people putting information on there that doesn't exist anywhere else."

Source: Richard A. Best, Jr., and Alfred Cumming," Open Source Intelligence (OSINT): Issues for Congress," December 5, 2007, RL34270, *CRS Report to Congress*, http://www.fas.org/sgp/crs/intel/RL34270.pdf

**Open Storage**
Storage of classified information within an accredited facility but not in General Services Administration approved secure containers, while the facility is unoccupied by authorized personnel.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Operation TIPS**
***See Terrorism Information Prevention System***

**Operational Documentation**

1. Visual information documentation of activities to convey information about people, places, and things. It is general purpose documentation normally accomplished in peacetime.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

2. *Operativnoye dokumentirovaniye*. Factual information detailing the subversive activities of intelligence officers and agents of capitalist intelligence services or anti-Soviet elements. Also the organizational aspects of the activities of state security agencies.

Source: Mitrokhin, Vasily, ed. *KGB Lexicon: The Soviet Intelligence's Officer's Handbook*. London: Frank Cass, 2002.

**Operational Files | Exemption**

1. Files "that document the means by which foreign intelligence or counterintelligence is collected through scientific and technical systems."

Source: War and National Defense. 50 U.S.C 403-5e, http://www.gpoaccess.gov/uscode/browse.html

2. National Reconnaissance Office told a federal court it should not have to process a Freedom of Information Act request for unclassified portions of its congressional budget justification book because the document is contained in "operational files" that are exempt from search and review under the FOIA.

That contention was challenged in a lawsuit by the Federation of American Scientists, which told the court that the budget book cannot be considered an operational file because it is disseminated inside and outside of the agency, and that records that have been disseminated are excluded by statute from the definition of operational files.

Source: FAS. Secrecy News. December 6, 2005, http://www.fas.org/sgp/news/secrecy/2005/12/index.html and Aftergood v. National Reconnaissance Office, http://www.fas.org/sgp/foia/nro-cbjb/index.html

3. Congress granted the Defense Intelligence Agency an exemption from the Freedom of Information Act for its "operational files," but only for the next two years. DIA is the fifth intelligence agency -- after CIA, NSA, NRO and NGA-- to receive such an exemption, which permits it to exclude from searching or reviewing for release under FOIA files "that document the conduct of foreign intelligence or counterintelligence operations."

Source: FAS. *Secrecy News* January 5, 2006, http://www.fas.org/sgp/news/secrecy/2006/01/010506.html, http://www.fas.org/sgp/foia/nro-cbjb/index.html, and FY 2006 Defense Authorization Act, accompanying report language, http://www.fas.org/sgp/congress/2005/dia-opfiles.html

4. Effective 21 April 2005, section 1071(a)(6) of the Intelligence Reform and Terrorism Prevention Act of 2004 amended the CIA Information Act, to provide that the Director of CIA (D/CIA), with the coordination of the Director of National Intelligence (DNI), may exempt CIA operational files from the FOIA search, review, publication, and disclosure provisions; and that not less than once every ten years, the D/CIA and the DNI shall review the exemptions in force, in order to make the determinations noted above.

The following categories of CIA operational files as exempt from the search, review, publication, and disclosure provisions of the FOIA. **Files within the Directorate of Operations** – Personality Files, External Organizations Files, Operational Interest Files, Operational Activity Files, Policy and Management Files (Including Clandestine Service History Program Files), Cover Arrangements Files; **Files within the Directorate of Science & Technology** – Signal Intelligence Activities Files, Operational and Technical Support Files, Intelligence Collections Systems Files, Imagery Analysis and Exploitation Files; **Files within the Security Center** – Covert Security Approval/SECRET Files, Provisional Covert Security Approval/SECRET Files, Operational Approval Files, Provisional Operational Approval Files, Anonymous Personnel Actions Files, Approval To Polygraph for Operational Purposes Files, Diversified Cover Officer Files, Contract/External Files, Covert Security Approval/SECRET Files, National Resources Division and Name Check/Operational Program Files, Industrial Special Security Approval/Covert, Industrial Security Approval/Covert, and Industrial Special Security Approval/Covert Reinvestigation Files, Internal/Covert Files, Consultant External/Operations and Consultant Internal/Operations Files.

Source: CIA. Report of the Second Decennial Review of CIA Operational File Exemptions. June 28, 2005. FAS, http://www.fas.org/sgp/othergov/ciaopf2.html

### Operational Information

Ridenour, according to Quist, Ridenour in 1945 was the first author to discuss the three classes of information – technical, scientific, and operational – that a government may want to classify as "subjective and objective information. " Operational information has the following properties of

- Compactness: "a few words can carry a great secret, therefore it is easy to steal."
- Universally understandable: "anyone can steal it."

- Arbitrary: “it therefore needs to be stolen; if the information consists of military information it is most likely “improbable and therefore has an element of surprise.”
- Subject to change
- Perishable: “Even the most stringent of security measures can be tolerated…as they are not permanent.”

Source: Louis Nicot Ridenour. "Military Security & the Atomic Bomb." *Fortune* November (1945): 32, 170-171, 216+, and Arvin S. Quist. Security Classification of Information. Volume 2. Principles for Classification of Information. April 1993, http://www.fas.org/sgp/library/quist2/chap_2.html

**Operations Research**

The analytical study of military problems undertaken to provide responsible commanders and staff agencies with a scientific basis for decision on action to improve military operations.

Source: Department of Defense. *DoD Dictionary of Military and Associated Terms*. JP 1-02. As Amended through 31 October 2009, http://www.dtic.mil/doctrine/dod_dictionary/ and Office of the Under Secretary of Defense. *Report of the Defense Science Board Advisory Group on Defense Intelligence Operations Research Applications for Intelligence, Surveillance and Reconnaissance (ISR),* January, 2009, http://www.fas.org/irp/agency/dod/dsb/or-intel.pdf

**Operations Security Protected Information**

Unclassified information concerning CDC mission, functions, operations, or programs that require protection in the national interest, security or homeland defense as iterated in National Security Decision Directive 298, January 1988, which established a National Operations Security Program.

Source: Centers for Disease Control. “Manual Guide - Information Security CD.C.-02.”
Office of Security and Emergency Preparedness “Sensitive But Unclassified Information.” 07/22/2005, http://www.fas.org/sgp/othergov/cD.C.-sbu.pdf.

**Opposing Information**

Intentional or unintentional truth-based information from any source that represents an opposing view.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**ORCON**

***See Dissemination and Extraction of Information Controlled by Originator | Classification Markings | Control Markings***

**Organizational History File**
Historical documents, photographs, and other items of significance to and belonging to a particular Army organization. (See AR 25-400-2.)

Source: Department of the Army. *Historical Activities, Military History: Responsibilities, Policies, and Procedures*, 21 September 2007, http://www.monmouth.army.mil/historian/reg/r870_5.pdf

**Original Classification**
***See Born Classified***

1. Information that meets the criteria and subject areas of EO 12356 or through unauthorized disclosure of the information "reasonably be expected to cause damage to national security."

Source: DOE. *Understanding Classification*. Washington, D.C.: U.S. Dept. of Energy, Assistant Secretary for Defense Programs, Office of Classification, 1987. SUDOC: E 1.15:0007/1

2. Original Classification is an initial determination by an authorized classifier that information requires extraordinary protection, because unauthorized disclosure of the information could reasonably be expected to cause damage to the national security. The process of original classification ordinarily includes both the determination of the need to protect the information and the placement of markings to identify the information as classified. By definition, original classification precedes all other aspects of the security classification system, e.g., derivative classification, safeguarding and declassification.

Source: ISOO. "2001 Annual Report to the President." http://www.archives.gov/isoo/reports/2001-annual-report.html

3. The initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. It is the act of deciding that information never classified before meets the criteria to be designated as classified information. Although the process of making original classification decisions can be complex and difficult, it consists of six steps (already classified, eligibility, damage, classification level, duration, communication of decision; chart, page 5 of NIMA Guide).

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

## Original Classification Authority

***See Equity***

1. Also called original classifiers; individuals designated in writing, either by the President or by selected agency heads, to classify information in the first instance. Under Executive Order 12958, as amended, only original classifiers determine what information if disclosed without authority could "reasonably be expected to cause damage to the national security." Original classifiers must be able to identify or describe the damage incurred from release of information. Approximately 4,000 officials hold original classification authority.

ISOO states "Because they are the only individuals in the process authorized to exercise discretion in making classification decisions, their decision to classify particular information constitutes the first stage in the life cycle of classified national security information and can spawn hundreds if not thousands of derivative classification decisions."

Source: Information Security Oversight Office (ISOO). 2004 Report to the President http://www.archives.gov/isoo/reports/2004-annual-report.html; for a list of OCAs, see FAS, Clinton EO 12958. http://www.fas.org/sgp/clinton/oca.html; Methodology for Determining Appropriateness of an Original Classification Decision http://www.archives.gov/isoo/pdf/appropriate-classification.pdf; and Memorandum for See Distribution, Standardized Methodology for Making Classification Decisions (2006?), http://www.fas.org/sgp/othergov/dod/methodology.pdf

## Original Classifier

An authorized individual in the executive branch who initially determines that particular information requires a specific degree of protection against unauthorized disclosure in the interest of national security and applies the classification designation "Top Secret," "Secret," or "Confidential."

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/

## Overclassification

1. Derivative decisions that cannot trace their origin or that improperly apply source guidance are a major source of overclassification.

Source: (Wright) Commission on Government Security, 1955, the (Stilwell) Department of Defense Security Review Commission, 1985, and the Commission on Protecting and Reducing Government Secrecy in 1997. http://www.fas.org/sgp/congress/2005/030205overclass.html; also see "Executive Order 12958, Amended," http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html.

2. Require that all finished intelligence products created by the Department be simultaneously prepared in the standard unclassified format, provided that such an unclassified product would reasonably be expected to be of any benefit to a State, local, tribal or territorial government, law enforcement agency or other emergency response provider, or the private sector, based on input provided by the Interagency Threat Assessment and Coordination Group Detail established under section 210D. (Sec. 210F, Overclassification Prevention Program).

Source: H.R.553 Reducing Over-Classification Act of 2009, *Congressional Record*, 155 (February 3, 2009), http://www.gpoaccess.gov/crecord/

**Overt Peacetime Psychological Operations Programs**
***See Psychological Operations***
Those programs developed by combatant commands, in coordination with the chiefs of US diplomatic missions, that plan, support, and provide for the conduct of psychological operations, during military operations other than war, in support of US regional objectives, policies, interests, and theater military missions.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Overt Products**
A product that openly identifies its source is known as an overt product. Overt products are disseminated and acknowledged by the originator or by an accredited agency thereof. They are disseminated without intention to deceive the target audience as to where they originated.

Source: DoD. Psychological Operations, FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

---

**~ P ~**

**PACER**
Public **A**ccess to **C**ourt **E**lectronic **R**ecords (PACER) is an electronic public access service that allows users to obtain case and docket information from Federal Appellate, District and Bankruptcy courts, and the U.S. Party/Case Index via the Internet. Each court maintains its own databases with case information. Because PACER database systems are maintained within each court, each jurisdiction will have a different URL. Accessing and querying information from each service is comparable; however, the format and content of information provided may differ slightly.

PACER is a service of the United States Judiciary. The PACER Service Center is run by the Administrative Office of the United States Courts. PACER is not free, but cheaper than an individual Westlaw or Lexis Nexis account (perhaps; see http://pacer.psc.uscourts.gov/faq.html#GP8).

Source: United States Judiciary, http://pacer.psc.uscourts.gov/pacerdesc.html

**Paperwork Reduction Act** [48]

The purposes of this subchapter are to--

(2) ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government;

(3) coordinate, integrate, and to the extent practicable and appropriate, make uniform Federal information resources management policies and practices as a means to improve the productivity, efficiency, and effectiveness of Government programs, including the reduction of information collection burdens on the public and the improvement of service delivery to the public;

(5) minimize the cost to the Federal Government of the creation, collection, maintenance, use, dissemination, and disposition of information;

(7) provide for the dissemination of public information on a timely basis, on equitable terms, and in a manner that promotes the utility of the information to the public and makes effective use of information technology;

(8) ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to--

(9) ensure the integrity, quality, and utility of the Federal statistical system;

---

[48] According to Blum, (1; Secrecy Report Card 2005. http://www.openthegovernment.org/otg/SRC2005.pdf)) in 2004, every document classified cost the government $460 to secure; shouldn't the PRA extend  to the expense of classifying docs?

(10) ensure that information technology is acquired, used, and managed to improve performance of agency missions, including the reduction of information collection burdens on the public;

Source: Paperwork Reduction Act. 44 USC 35 § 3501, http://www.archives.gov/federal-register/laws/paperwork-reduction/3501.html

2. The PRA requires that agencies obtain OMB approval for collections of information. A collection of information without current OMB approval constitutes a violation of the PRA. Each year OMB is required to report to Congress PRA violations published in the Information Collection Budget of the United States.

Source: Office of Management and Budget. "Fiscal Year 2005 Information Collection Budget." OMB Bulletin 04-04. September 28, 2004, http://www.whitehouse.gov/omb/bulletins/fy04/b04-04.pdf

**Partition | Partitioning**

***See Informational In-Breeding***

Partitioning is the act of territorially containing and restricting access to information based on its perceived importance. Partitioning is accomplished via codes, code-words, symbols, filing practices, access clearances, markings, subdivisions, categories, caveats, and imposition of agency-specific controls over information. Partitioning is best represented in the bureaucracy[49], and has its roots in Weber's (1978: 988) idea of the files wherein,

> Increasingly all order in public and private organizations is dependent on the system of files and the disciplines of officialdom, that means, its habit of painstaking obedience within its wonted sphere of action.

[49] Max Weber (1968: 223) writes that "From a purely technical point of view, a bureaucracy is capable of attaining the highest degree of efficiency, and is in this sense formally the most rational known means of exercising authority over human beings. It is superior to any other form in precision, in stability, in the stringency of its discipline, and in its reliability. It thus makes possible a particularly high degree of calculability of results for the heads of the organization and for those acting in relation to it. It is finally superior both in intensive efficiency and in the scope of its operations and is formally capable of application to all kinds of administrative tasks." *Max Weber on Law in Economy and Society*. (Trans. Edward Shils and Max Rheinstein. Ed. Max Rheinstein. New York: Simon and Schuster, 1968).

In the process of manufacturing and systematizing information from its various channels, codes, functions and products, partitioning of information serves to legitimate certain types of information access and practices while diminishing others. An example of partitioning is that of "informational in-breeding," wherein information can be shared only with those on the same "secret island" who hold similar privilege (Hourcle 316). To my knowledge, "partition" has never been used in the way I intend.

Source: Definition, Maret; *Max Weber. Economy and Society: An Outline of Interpretive Sociology.* Trans. Ephraim Fischoff. Ed. Guenther Roth and Claus Wittich. Berkeley: University of California Press, 1978, and Laurent R. Hourcle. "Military Secrecy and Environmental Compliance." *New York University Environmental Law Journal* 2 no. 2 (1993): 316-346, http://www1.law.nyu.edu/journals/envtllaw/issues/vol2/index.html

**Partitioned Security Mode**

Information system (IS) security mode wherein all personnel have the clearance, but not necessarily formal access approval and need-to-know, for all information handled by an IS.

Source: Committee for National Security Systems (CNSS). Instruction 4009. National Information Assurance Glossary, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Passenger Name Record**

*See Secure Flight*

A record that contains detailed information about an individual's travel on a particular flight, including information provided by the passenger when making the flight reservation. Though the content of PNRs varies among airlines, PNRs may include, among other information: (1) Passenger name; (2) reservation date; (3) travel agency or agent; (4) travel itinerary information; (5) form of payment; (6) flight number; and (7) seating location.

(Page 10 of http://www.dhs.gov/interweb/assetlibrary/CBP-DHS_PNRUndertakings5-25-04.pdf lists data elements that must be reported by air carriers to the Department of Homeland Security Bureau of Customs and Border Protection (CBP)).

The European Court of Justice (ECJ) struck down a passenger name record deal that allowed the transfer of personal information on European travelers to the U.S.
government, as no accord was struck by the court-appointed deadline of September 30.

Source: DHS. TSA. "Reports, Forms, and Recordkeeping Requirements: Agency Information Collection Activity Under OMB Review; Secure Flight Test Phase," *Federal Register* 69(185): September 24, 2004; Electronic Privacy Information Center (EPIC). "EU-US Airline Passenger Data Disclosure," http://www.epic.org/privacy/intl/passenger_data.html; William J. Krouse. "Terrorist Watchlist Checks and

Air Passenger Prescreening." *CRS Report to Congress* September 6, 2006, http://www.fas.org/sgp/crs/homesec/RL33645.pdf; EPIC, Ruling of the European Court of Justice. http://www.epic.org/redirect/ec_court_passenger.html and DHS, Statement by Homeland Security Secretary Michael Chertoff on Passenger Name Record Agreement with European Union

**Pass/Fail**

A declassification technique that regards information at the full document or folder level. Any exemptible portion of a document or folder may result in exemption (failure) of the entire documents or folders. Documents or folders that contain no exemptible information are passed and therefore declassified. Documents within exempt folders
are exempt from automatic declassification. Declassified documents may be subject to FOIA exemptions other than the security exemption ((b) (1)), and the requirements placed by legal authorities governing Presidential records and materials.

Source: National Defense. 32 CFR 2001, http://www.gpoaccess.gov/CFR/index.html.

**Patent(s)**

A patent for an invention is the grant of a property right to the inventor, issued by the United States Patent and Trademark Office. Generally, the term of a new patent is 20 years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. U.S. patent grants are effective only within the United States, U.S. territories, and U.S. possessions. Under certain circumstances, patent term extensions or adjustments may be available.

There are three types of patents: 1) Utility patents may be granted to anyone who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof; 2) Design patents may be granted to anyone who invents a new, original, and ornamental design for an article of manufacture; and 3) Plant patents may be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant.

Source: U.S. Patent and Trademark Office. "General Information Concerning Patents." http://www.uspto.gov

**PATHFINDER**

***See Data Mining***

Defense Intelligence Agency. Is a data mining tool developed for analysts that provides the ability to analyze government and private sector databases rapidly. It can compare and search multiple large databases quickly;

Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. Data Mining: Federal Efforts Cover a Wide Range of Uses. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Pen Register**

Section 3127(3) of Title 18, United States Code, is amended--
(A) by striking "electronic or other impulses" and all that follows through "is attached" and inserting "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication"; and
(B) by inserting "or process" after "device" each place it appears.

Source: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2000, section 216, http://purl.access.gpo.gov/GPO/LPS17579

**People Access Security Service (PASS)**

1. Mandated by the Intelligence Reform and Terrorism Prevention Act of 2004, "the passport card is intended as a lower cost means of establishing identity and nationality for American citizens in two limited situations--for citizens crossing U.S. land borders and traveling by sea between the U.S., Canada, Mexico, the Caribbean or Bermuda."

Source: State Department's Federal Register PASS Card Proposal, *Federal Register* 71 no. 200 (October 17, 2006): 60928-60932, http://access.gpo.gov

2. Accepted documents for U.S. citizens will be either a valid U.S. passport or the proposed People Access Security Service (PASS) card, which, if adopted as proposed, would include a long-range wireless technology that would create an increased security risk. This is a significant change from the previous system, where U.S. citizens would show a driver's license, birth certificate or nothing at all to cross the border.

Source: Electronic Privacy Information Center (EPIC). "Homeland Security PASS Card: Leave Home Without It," Spotlight on Surveillance, August 2006, http://epic.org/privacy/surveillance/spotlight/0806/

**Perception Management**

***See Psychological Operations***

Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/ and Joint Publication 3-53. *Doctrine for Joint Psychological Operations*. September 5, 2003, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53.pdf

**PERSEREC Database**

Since 1987, the Defense Personnel Security Research Center (PERSEREC) has maintained a database on espionage by American citizens based largely on open sources, and has collected files on each of the 173 individuals in the database. Espionage by Americans is the worst outcome for the personnel security system that works to reduce the risk of insider threat. Although its main focus is the personnel security system, PERSEREC monitors and analyzes espionage by Americans in order to improve understanding of this betrayal of trust by a small minority of citizens. The *PERSEREC espionage* database is based on open source information.

Source: Katherine L. Herbig, *Changes in Espionage by Americans: 1947-2007*, Technical Report 02-05, March 2008, http://www.dhra.mil/perserec/reports.html

**Personally Identifiable Information**

1. Generally, privacy interests cognizable under the FOIA are found to exist in such personally identifying information as a person's name, address, phone number, date of birth, criminal history, medical history, and social security number.34

Source: Department of Justice, FOIA Guide, "Exemption 6," and footnote #34, 2009 http://www.justice.gov/oip/foia_guide09/exemption6.pdf

2. PII has become the generally accepted language; ALA began using this term in 1991 when it adopted the Policy Concerning Confidentiality of Personally Identifiable Information about Library Users PII connects individuals to what they bought with their credit cards, what they checked out with their library cards, and what Web sites they visited where they picked up cookies. More than simple identification, PII can build up a picture of tastes and interests—a dossier of sorts, though crude and often inaccurate. While targeted advertising is the obvious

use for PII, some people would use this information to assess an individual's character, decide if they were a security risk, or embarrass them for opposing a particular position. Because of the chilling effect that such scrutiny can have on open inquiry and freedom of expression, libraries and bookstores have long resisted requests to release information that connects individual persons with specific books.

Source: American Library Association. "Guidelines for Developing a Library Privacy Policy," 2005, http://tinyurl.com/yg5779f

### Physical Security Codes

*See Critical Nuclear Weapons Design Information, Security Clearances*

According to DoD 5160.65-M, "security aspects of conventional ammunition life-cycle management. It covers policies and procedures for physical security, information security, exchanging security information, and categorizing security risks for sensitive ammunition and explosives. Physical security policies and procedures are designed for maximum uniformity and standardization. Although they are aimed at securing the DoD conventional ammunition PB, they are adaptable to the special needs of the individual Military Services."

The following codes indicate "the degrees of protection required for materials in the interest of national security:"

Code A: Confidential Formerly Restricted Data

Requires L Clearance

Code B: Confidential Restricted Data

The lowest classification level applied to information whose unauthorized disclosure could reasonably be expected to cause damage to the national security.
Requires L Clearance.

- Code C (Confidential)
- Code D: Confidential Cryptologic
- Code E  Secret Cryptologic
- Code F: Top Secret Cryptologic
- Code G: Secret Formerly Restricted Data

Requires L Clearance.

- Code H: Secret Restricted Data
- Code K: Top Secret Formerly Restricted Data
- Code L: Top Secret Restricted Data.

Requires Q Clearance.

- Code S: Secret

- Code T: Top Secret
- Code U: Unclassified

Source: DoD 5160.65-M "Single Manager for Conventional Ammunition (Implementation Joint Conventional Ammunition Policies and Procedures)", 04/1989." Chapter 12 Table 12-11, http://www.dtic.mil/whs/directives/corres/pdf/516065m_0489/chap12.pdf

**Pink Paper**

***See Blue Paper***

To distinguish these more sensitive informal memoranda from official memoranda that were to be serialized and indexed in the FBI's central records system, an informal memorandum was to be written on pink paper (official memoranda were written on white paper) and to contain the notation that the memorandum was "to be destroyed after action is taken and not sent to files."

Source: Athan Theoharis, ed. *The FBI: A Comprehensive Reference Guide*. Phoenix: Oryx Press, 1998. 22.

**Plain Text**

Unencrypted information.

Source: Committee for National Security Systems (CNSS). Instruction 4009. National Information Assurance Glossary, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Pointer System or Index**

A system that stores information designed to identify individuals, organizations, and/or crime methodologies with the purpose of linking law enforcement agencies that have similar investigative and/or intelligence interests in the entity defined by the system.

Source: DOJ, Global Justice Information Sharing Initiative, Criminal Intelligence Glossary of Terms, Minimum Criminal Intelligence Training Standards, Appendix, October 2007, http://www.it.ojp.gov/documents/min_crim_intel_stand.pdf

**Plan Information Capability**

The capability that allows a supported command to enter and update key elements of information in an operation plan stored in the Joint Operation Planning and Execution System.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Police Information**

The products from the collection, analysis, and interpretation of all available information concerning known and potential enemy and criminal threats and vulnerabilities of support organizations. It involves intelligence preparation of the battlefield, criminal intelligence preparation of the battlefield, and the police information assessment process.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. Operational Terms and Graphics. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Possible**

Information or intelligence reported by only one independent source is classified as "possibly true." The test for independence is certainty that the information report of a source was not derived from some other source, usually resulting in reliance on original reporting. A classification of "possibly true" cannot be based on analytical judgment alone.

Source: Department of the Army. FM 34-1. Glossary. Intelligence and Electronic Warfare Operations. September 1994, http://www.fas.org/irp/doddir/army/fm34-1/gloss.htm#GLOSS

**Power Projection**

The ability of a nation to apply all or some of its elements of national power—political [Note: the Army replaces "political" with "diplomatic" in this newer version of the definition], economic, informational, or military—to rapidly and effectively deploy and sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. Operational Terms and Graphics. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Power to the Edge**

***See Agility***

1. Power to the Edge principles, particularly those that involve increasing the ability of the edge to understand and act, are related to agility. In fact, Power to the Edge states that "edge organizations have the attributes to be agile. This is because agility requires that available information is combined in new ways, that a variety of perspectives are brought to bear, and that assets can be employed differently to meet the needs of a variety of situations" (page 217).

Source: Simon Reay Atkinson and James Moffat *The Agile Organization: From Informal Networks to Complex Effects and Agility*, DoD, CCRP, 2005, (p. xxi),

http://www.dodccrp.org/files/Atkinson_Agile.pdf

2. Power to the edge is about changing the way individuals, organizations, and systems relate to one another and work. Power to the edge involves the empowerment of individuals at the edge of an organization (where the organization interacts with its operating environment to have an impact or effect on that environment) or, in the case of systems, edge devices. Empowerment involves expanding access to information and the elimination of unnecessary constraints. (p. 4-5)

Source: David S. Alberts and Richard E. Hayes *Power to the Edge Command, Control, in the Information Age*, DoD, CCRP 2003, http://www.dodccrp.org/html4/books_downloads.html

**Practical Obscurity** [50]

1. The "practical obscurity" concept expressly recognizes that the passage of time may actually increase the privacy interest at stake when disclosure would revive information that was once public knowledge but has long since faded from memory.

Source: DOJ. FOIA Guide, Exemption 7c, 2009, pp.578-579.
http://www.justice.gov/oip/foia_guide09/exemption7c.pdf

2. But the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.

Source: Jusitce Stevens, *United States Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749 (1989),
http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&vol=489&invol=749 and Nancy S. Marder, "From 'Practical Obscurity'" to Web Disclosure: A New Understanding of Public Information,"59 *Syracuse L. Rev.* 441 (2009).

**Practical Utility**

***See Burden***

The actual, not merely the theoretical or potential, usefulness of information to or for an agency, taking into account its accuracy, validity, adequacy, and reliability, and the agency's ability to process the information it collects (or a person's ability to receive and process that which is disclosed, in the case of a third-party or public disclosure) in a useful and

[50] Thanks to SLIS SJSU grad student Anne Sawucki for bringing this concept to my attention.

timely fashion. In determining whether information will have “practical utility," OMB will take into account whether the agency demonstrates actual timely use for the information either to carry out its functions or make it available to third-parties or the public, either directly or by means of a third-party or public posting, notification, labeling, or similar disclosure requirement, for the use of persons who have an interest in entities or transactions over which the agency has jurisdiction. In the case of recordkeeping requirements or general purpose statistics (see Sec. 1320.3(c) (3)), “practical utility" means that actual uses can be demonstrated.

Source. Office of Management and Budget. 5 CFR 1320. “Controlling Paperwork Burdens on the Public.” http://www.gpoaccess.gov/cfr/index.html

**Precautionary Principle**

1. When an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically. In this context the proponent of an activity, rather than the public, should bear the burden of proof. The process of applying the Precautionary Principle must be open, informed and democratic and must include potentially affected parties. It must also involve an examination of the full range of alternatives, including no action.

Source: Wingspread Conference on the Precautionary Statement. January 26, 1998, http://www.sehn.org/wing.html

2. Precaution is at the basis of some U.S. environmental and food and drug legislation, although the principle is not mentioned by name. These laws incorporate foresight, prevention, and care, and many give regulators authority to take action to prevent possible but unproven harm. For example:

- As a precautionary measure, the Food and Drug Administration requires all new drugs to be tested before they are put on the market.
- The Food Quality and Protection Act of 1996 requires pesticides to be proven safe for children or removed. Several are being phased out.
- The National Environmental Policy Act is precautionary in two ways: 1) It emphasizes foresight and attention to consequences by requiring an environmental impact assessment for any federally funded project, and 2) it mandates consideration of alternative plans. NEPA is one of the best national examples of precautionary action.

Source: Science and Environmental Health Network. “Precautionary Principle FAQ. “ http://www.sehn.org/ppfaqs.html

**Prepackaged News**[51]

***See Propaganda, Smith-Mundt Act of 1948***

Also termed "fake news."

1. Prepackaged news stories are complete, audio-video presentations that may be included in video news releases, or VNRs. They are intended to be indistinguishable from news segments broadcast to the public by independent television news organizations. To help accomplish this goal, these stories include actors or others hired to portray "reporters" and may be accompanied by suggested scripts that television news anchors can use to introduce the story during the broadcast. These practices allow prepackaged news stories to be broadcast, without alteration, as television news.

The publicity or propaganda prohibition states, "No part of any appropriation contained in this or any other Act shall be used for publicity or propaganda purposes within the United States not heretofore authorized by the Congress." GAO has long interpreted this provision to prohibit agencies from, among other things, producing materials that are covert as to origin. Our opinions have emphasized that the critical element of covert propaganda is concealment of the government's role in producing the materials. Agencies have violated this law when they used appropriated funds to produce articles and op-ed pieces that were the ostensible position of persons not associated with the government.

In two legal opinions this past year, federal agencies commissioned and distributed prepackaged news stories and introductory scripts about their activities that were designed to be indistinguishable from news stories produced by private news broadcasters. In neither case did the agency include any statement or other indication in its news stories that disclosed to the television viewing audience, the target audience of the purported news stories, that the agency wrote and produced those news stories. In other words, television-viewing audiences did not know that stories they watched on television news programs about the government were, in fact, prepared by the government. GAO concluded that those prepackaged news stories violated the publicity or propaganda prohibition.

Source: U.S. General Accountability Office. "Video News Releases: Unattributed Prepackaged News Stories Violate Publicity or Propaganda Prohibition." [GAO-05-643T. May 12, 2005, http://www.gao.gov/htext/d05643t.html] and Center for Media and Democracy, Diane Farsetta and Daniel Price,"Still Not the News: Stations Overwhelmingly Fail to Disclose VNRs." November 14, 2006, http://www.prwatch.org/fakenews2/execsummary

[51] There are parallels in U.S. history with the WWI Creel Commission (Committee on Public Information (CPI) ), and USIA, for example, see Nancy Snow's various works.

2. SEC. 821. No part of any funds appropriated in this or any other Act shall be used by an agency of the executive branch, other than for normal and recognized executive-legislative relationships, for publicity or propaganda purposes, and for the preparation, distribution or use of any kit, pamphlet, booklet, publication, radio, television or film presentation designed to support or defeat legislation pending before the Congress, except in presentation to the Congress itself.

Source: "Making Appropriations for the Departments of Transportation, Treasury, and Housing and Urban Development, the Judiciary, District of Columbia, and independent agencies for the fiscal year ending September 30, 2006, and for other purposes." 109 P.L. 115; 119 Stat. 2396; 2005 Enacted H.R. 3058; 109 Enacted H.R. 3058. November 30, 2005, http://www.gpoaccess.gov/plaws/

3. The Government Accountability Office has scored the Office of National Drug Control Policy and the Education and Health and Human Services departments, among others, for spending millions of dollars on prepackaged news stories designed to mimic TV newscasts and for paying popular pundits for positive media treatment. In several reports issued since 2004, GAO accused some agencies of engaging in illegal "covert propaganda" for producing video news releases that did not identify who produced them.

But agencies can continue to use video news releases so long as they disclose their origin — and they do. Last year, the Interior Department produced one starring Clint Eastwood to help launch a campaign to improve public parks and wildlife refuges. In recent years, agencies have used them to promote highway safety and warn against consumer scams and unpasteurized juices, GAO noted. Federal officials and experts say that as agencies launch new public relations programs, they must be careful not to emphasize image over substance and results.

Source: Mollie Ziegler. "Critics say corporate-style PR goes too far." August 30th, 2006, http://federaltimes.com/index.php?S=2060330

**Also see**: 9/24/07 Press Release, Commissioner Adelstein Applauds (Comcast) Enforcement Bureau VNR Decision, http://www.fcc.gov/commissioners/adelstein/pressreleases.html

**Prepublication Review**

***See Non Disclosure Agreement***

1. Reagan National Security Decision Directive 84, "Safeguarding National Security Information," March 11, 1983;

> All present Compartmented Information be required to sign a nondisclosure agreement as a condition of access to SCI and other classified information, and that this particular

agreement must include a provision for prepublication review of writing for public consumption to assure deletion of SCI and other classified information:

Source: NSDD 84. "Safeguarding National Security Information."
http://www.fas.org/irp/offdocs/nsdd/nsdd-084.htm

2. The prepublication review agreement requited by NSDD 84, was, in fact, a revised version of the CIA's Form 4193. Unknown to Congress, the Reagan administration had already been using the CIA's lifetime censorship contract Form 4193, as a "boilerplate" secrecy contract throughout the government. The General Accounting Office reported at the end of 1983, excluding the CIA and the National Security Agency, 23 agencies had required 119,000 employees to sign Form 4193.

Prepublication review agreements in academia revisit the controls imposed by President Reagan under NSDD 84. The directive's provisions for lifetime prepublication review applied to university researchers because certain research grants are government sponsored. The practice of using prepublication review in science-related government grants has led to a trend in other government-sponsored university research contracts in areas involving neither military nor classified information.

Source: Steven L. Katz. *Government Secrecy: Decisions without Democracy*. Washington, D.C.: People for the American Way, 1987. 31-34, 42; also see CIA, "Agency Prepublication Review of Certain Material Prepared for Public Dissemination," May 2007, http://www.fas.org/irp/cia/prb2007.pdf

3. All government employees with high security clearances are required to sign "Form 4193" which contains a lifetime promise to submit for prepublication review all writings, including works of fiction. Nondisclosure Agreements and H.R. 4392, the "Intelligence Authorization Act for Fiscal Year 2001" (popularly known as the "Official Secret Act") punishes federal employees for disclosing classified information. [52] This is a lifetime agreement.

Source: United States. Congress. House. Committee on the Judiciary. Subcommittee on Civil and Constitutional Rights. *Presidential Directive on the Use of Polygraphs and Prepublication Review* : Hearings before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, Ninety-eighth Congress, first and second sessions ... April 21, 28, 1983, and February 7, 1984 Publisher Washington : GPO, 1985. Y 4.J 89/1:98/114

[52] Kate Martin, director of the Center for National Security Studies believes the Act is unconstitutional and "sanctions for disclosure already exist." The Act also, ignores public debate and poses a risk to freedom of the press. @ FAS http://www.fas.org/sgp/news/2000/09/leaks.html

4. CIA: Performed by the CIA's Publications Review Board (PRB) and federal courts "have approved the process, which stems from the DCI's statutory obligation to protect sources and methods." According to Hedley, "the sole purpose of prepublication review is to assist authors in avoiding inadvertent disclosure of classified information which, if disclosed, would be damaging to national security--just that and nothing more."

Source: John Hollister Hedley. "Reviewing the Work of CIA Authors: Secrets, Free Speech, and Fig Leaves." https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/spring98/Secret.html ; also see Ralph W. McGhee's "Appendix: This Book and the Secrecy Agreement," *Deadly Deceits: My 25 Years in the CIA*. New York: Sheridan Square Publications, 1983, and CIA. "Agency Prepublication Review of Certain Material Prepared for Public Dissemination." July 22, 2005, http://www.fas.org/irp/cia/prb2005.pdf

5. Department of State. Not termed 'Prepublication Review" but *de facto* acts as such:

Official appearances before the media or general public to give formal interviews, speeches, or remarks must be cleared with the Assistant Secretary for Public Affairs. See 3 FAM. See 10 FAM 121.4.

All unofficial speaking, writing, or teaching activities which are of official concern must be approved by the Assistant Secretary for Public Affairs, in accordance with 3 FAM. See 10 FAM 121.4.

Former employees remain obligated by law not to disclose classified information, and certain employees may be bound by non-disclosure agreements. See also 3 FAM *628.2a*-c.

Source: Department of State. *Foreign Affairs Manual*. 10 FAM 120 & 120.2, "Remarks and Writings for the Media and General Public." http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents and *Weaver v. United States Information Agency*. 520 U.S. 1251; 117 S. Ct. 2407; 138 L. Ed. 2d 174; 1997 U.S. LEXIS 3405; 65 U.S.L.W. 3798; 12 I.E.R. Cas. (BNA) 1568, June 2, 1997, Decided.

6. Department of Defense (DoD) has been among the first government departments to take the lead in spelling out rules for what should and should not go on a web site and how information should be reviewed before it is posted on a web site.

Source: Defense Security Service. "Pre-Publication Review of Website Content."[See Wayback Machine, http://web.archive.org/web/20060220114841/http://www.dss.mil/search-dir/training/csg/security/S2unclas/Website.htm ]

7. National Security Agency | Central Security Agency:

**Why a pre-publication review?**

All NSA/CSS affiliates (past and present) are responsible for forwarding for review any information intended for public disclosure which is or may be based on protected information gained while associated with NSA/CSS.

Note: Public disclosure means disclosure to one or more persons who do not have the appropriate access authorization, security clearance and/or need-to-know to receive protected information.

**Who must submit materials intended for publication to NSA/CSS for review?**

Pre-publication review responsibilities are the same whether you are an NSA/CSS employee, a contractor, a military member or other affiliate who has had access to NSA/CSS information or facilities. Included in this sort of information is any work that relates to the Intelligence Community in general, such as spy novels. Publications about gardening, cooking, sports, crafts, etc. do not need to undergo pre-publication review ***unless*** mention of the author's affiliation with NSA/CSS is included.

Reminder: Pre-publication review is a lifetime responsibility. Your responsibility does not end when you end your association with NSA/CSS.

Source: National Security Agency | Central Security Agency. [See the Wayback Machine http://web.archive.org/web/20080211063422/http://www.nsa.gov/public/publi00010.cfm]

8. Justice Stevens, in the dissenting opinion in the prepublication review case *Snepp v. United States* wrote:

The mere fact that the Agency has the authority to review the text of a critical book in search of classified information before it is published is bound to have an inhibiting effect on the author's writing. Moreover, the right to delay publication until the review is completed is itself a form of prior restraint that would not be tolerated in other contexts.

Source: *Snepp v. United States* 444 *U.S.* 507 (1980), footnote 17. http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=444&invol=507; Andrew R. Sommer, "Casenote: The State Secrets Privilege in Prepublication Review: Proposing a Solution to Avoid a Seemingly Inevitable Tragedy." *George Mason Law Review* Fall, 2003 (12 Geo. Mason L. Rev. 211); Angus Mackenzie. *Secrets: The CIA's War at Home.* University of California Press, 1997, Jonathan C. Medow, "The First Amendment and the Secrecy State: *Snepp V. United States*," *University of Pennsylvania Law Review* 130 no.4 (1982): 775-844, and *Robert G. Wright v. Federal Bureau of Investigation*, (*Fatal Betrayals* manuscript) http://www.fas.org/sgp/jud/wright050609.pdf.

**Presidential Advance Manual**

There are several ways the advance person can prepare a site to minimize demonstrators. First, as always, work with the Secret Service and have them ask the local police department to designate a protest area where demonstrators can be placed, preferably not in view of the event site or motorcade route. The formation of "rally squads" is a common way to prepare for demonstrators by countering their message. This tactic involves utilizing small groups of volunteers to spread favorable messages using large hand held signs, placards, or perhaps a long sheet banner, and placing them in strategic areas around the site. These squads should be instructed always to look for demonstrators. The rally squad's task is to use their signs and banners as shields between the demonstrators and the main press platform. If the demonstrators are yelling, rally squads can begin and lead supportive chants to drown out the protestors (USA!, USA!, USA!). (p.34)

Source: ACLU, "White House Policy Illegally Silences Americans Critical of Bush," http://www.aclu.org/freespeech/protest/silenced.html and Peter Baker, "White House Manual Details How to Deal With Protesters," Washington Post August 22, 2007, http://tinyurl.com/ykof6rf

**Presidential Decision Directives**

***See Presidential Directive***

1. There are several types of PDDs, each determined and expanded on by individual presidential administrations beginning with Truman administration. PDDs are not publicly disclosed or published (as for example Executive Orders are published in the *Federal Register* and *Code of Federal Regulations*), or revealed to Congress. PDDs remain in effect until they are superseded by a new presidential administration. PDDs may be considered a "presidential secret law. "

Source: FAS Project on Government Secrecy, http://www.fas.org/irp/offdocs/direct.htm

2. Presidential Decision Directive (PDD) series is used to promulgate Presidential decisions on national security matters.

Source: FAS. Presidential Decision Directives. Clinton Administration 1993-2000, http://www.fas.org/irp/offdocs/pdd/index.html

3. A GAO study found that since 1961, only 247 of the Directives were publicly released out of the 1,042 PDDs that were issued by various presidential administrations. Of the 247 PDDs, GAO found that 116, "or about half of the 247…fell into three identified categories -- they established policy, directed the implementation of policy, and/or authorized the commitment of government resources. "

Source: General Accounting Office. *National Security: the Use of Presidential Directives to Make and Implement U.S. Policy: Report to the Chairman, Committee on Government Operations, House of Representatives*. Washington, D.C., 1988. http://www.gao.gov and General Accounting Office. *The Use of Presidential Directives to Make and Implement U.S. Policy.* NSIAD-92-72, January 1992, http://www.gao.gov

**Presidential Determination**

***See Presidential Finding***

1. Since the enactment of the Foreign Assistance Act in 1961, special authorities have been in effect; each use of the special authorities is conditioned on a determination or certification by the President. The implementing procedure is known as a Presidential Determination (PD). The President has never delegated the authority to invoke these special authorities. Overall responsibility for recommending that the President invoke a special authority was transferred from the Agency for International Development in 1968 to the State Department.

A Presidential Finding or Determination is a document signed by the President determining and authorizing use of an authority [such as "cloaking"]. Generally, this is accompanied by documents supporting and justifying authority. (46).

Source: General Accounting Office. "Use Of Special Presidential Authorities For Foreign Assistance. " GAO INSIAD-05-79. May 20, 1985, http://www.gao.gov (lists PDs from the 1960s).

2. According to Relyea, Determinations, "as a particular type of administrative order," first appeared in the *Federal Register* and *Code of Federal Regulations* (CFR) in 1964.

Source: Harold C. Relyea. "President Directives: Background and Overview." January 7, 2005. http://www.fas.org/irp/crs/98-611.pdf; also see "The President's Constitutional Authority to Conduct Military Operations against Terrorists and Nations Supporting Them." September 25, 2001, http://www.fas.org/irp/agency/doj/olc092501.html; United States. Congress. House. Committee on Government Operations. Special Subcommittee on Government Information. *Availability of Information from Federal Departments and Agencies.* Part 8. Department of Defense. (Hearings before the United States House Committee on Government Operations, Special Subcommittee on Government Information, Eighty-Fifth Congress, first session, on Mar. 11, 12, 1957. Washington: GPO, 1957. SUDOC: Y4.G 74/7: IN3/pt.8), and 3 U.S.C 4 § 301.

Determinations may be located at the U.S. Department of State Website, http://www.state.gov/

**Presidential Directive**

***See* National Security Decision Directive**, *National Security Presidential Directive*

A presidential directive has the same substantive legal effect as an executive order. It is the substance of the presidential action that is determinative, not the form of the document conveying that action. Both an executive order and a presidential directive remain effective upon a change in administration, unless otherwise specified in the document, and both continue to be effective until subsequent presidential action is taken.

Source: Department of Justice. "Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order." January 29, 2000. http://www.usdoj.gov/olc/predirective.htm; for a list of PDs, see FAS, Project on Government Secrecy. http://www.fas.org/irp/offdocs/nsdd/index.html; Harold C. Relyea. "President Directives: Background and Overview." January 7, 2005. http://www.fas.org/irp/crs/98-611.pdf, George Caldwell. "Presidential Directives and Where to Find Them." Library of Congress, http://www.loc.gov/rr/news/directives.html and Harold C. Relyea, "Presidential Directives: Background and Overview," Updated April 23, 2007, *CRS Report to Congress,* http://www.fas.org/irp/crs/98-611.pdf

**Presidential Finding**

***See Presidential Determination***

1. A Presidential authorization or directive based on an investigation for covert action, in which the President "finds" covert activities critical to national security. A finding may not may not authorize or sanction a covert action, or any aspect of any such action, which already has occurred, nor authorize any action that would violate the Constitution or any statute of the United States.

Source: War and National Defense. 50 U.S.C. Sec. 413b. http://www.gpoaccess.gov/U.S.C.ode/

2. Can include political activity, secret use of propaganda, economic disruption, paramilitary operations,; formalized covert action by requiring the President to inform Congress in writing (the Hughes-Ryan Act of 1974 which required the President to report any non-intelligence CIA operations such as covert operations to relevant Congressional committee (around 8 congressional committees at the time of the Act) in a timely fashion; the 1980 Intelligence Accountability Act which required only two committee be informed of the president's "finding."

Source: Leonard W. Levy and Louis Fisher, eds., *Encyclopedia of the American Presidency*. New York: Simon & Schuster, 1994.

**Presidential Records**

If a President, prior to the conclusion of his term of office or last consecutive term of office, as the case may be, specifies durations, not to exceed 12 years, for which access to certain information contained in Presidential records shall be restricted, in accordance with 44 U.S.C.

2204, the Archivist or his designee shall identify the Presidential records affected, or any reasonably segregable portion thereof, in consultation with that President or his designated representative(s).

Source: NARA. 36 CFR 1270.40, http://www.gpoaccess.gov/CFR/index.html

### Presidential Restrictions

The Presidential Records Act (PRA) establishes that eight of the nine FOIA exemptions shall apply to Presidential records, which stay in effect after the Presidential restrictions expire. Congress specifically excluded Presidential records from the FOIA (b) (5) exemption concerning the deliberative process and other recognized privileges. Four of the six presidential restrictions are identical to corresponding FOIA exemptions: exemptions 1, for classified national security information; exemptions 3, for information protected by other statute; exemptions 4, for trade secrets and confidential business information; and exemptions 6, for unwarranted invasions of personal privacy. Presidential exemption 2 ("P2"), for "appointments to Federal office," has no FOIA counterpart, but is subsumed, in large part, under FOIA exemption (b) (6). Presidential exemption 5 ("P5"), concerning "confidential communications requesting or submitting advice, between the President and his advisers, or between such advisers," is similar to FOIA exemption (b)(5), and protects the disclosure of presidential communications, deliberations, and other information that could be subject to a common law or constitutionally-based privilege.

Source: John W. Carlin. "On the Implementation and Effectiveness of the Presidential Records Act of 1978." November 6, 2001. http://www.archives.gov/presidential-libraries/laws/access/pra-1978.html and Presidential Records Act of 1978 and "Presidential Records Act Executive Order
Further Implementation of the Presidential Records Act Executive Order." November 1, 2001 [See the Wayback Machine,
http://web.archive.org/web/20071214203059/http://www.whitehouse.gov/news/releases/2001/11/20011101-12.html

### Presidential Signing Statements

1. Many Presidents have used signing statements to make substantive legal, constitutional, or administrative pronouncements on the bill being signed. Although the recent practice of issuing signing statements to create "legislative history" remains controversial, the other uses of Presidential signing statements generally serve legitimate and defensible purposes.

We believe that such statements may on appropriate occasions perform useful and legally significant functions. These functions include (1) explaining to the public, and particularly to constituencies interested in the bill, what the President believes to be the likely effects of its adoption, (2) directing subordinate officers within the Executive Branch how to interpret or

administer the enactment, and (3) informing Congress and the public that the Executive believes that a particular provision would be unconstitutional in certain of its applications, or that it is unconstitutional on its face, and that the provision will not be given effect by the Executive Branch to the extent that such enforcement would create an unconstitutional condition.

These functions must be carefully distinguished from a much more controversial -- and apparently recent -- use of Presidential signing statements, i.e., to create legislative history to which the courts are expected to give some weight when construing the enactment. In what follows, we outline the rationales for the first three functions, and then consider arguments for and against the fourth function.(2) The Appendix to the memorandum surveys the use of signing statements by earlier Presidents and provides examples of such statements that were intended to have legal significance or effects.

In 1986, then-Attorney General Meese entered into an arrangement with the West Publishing Company to have Presidential signing statements published for the first time in the *U.S. Code Congressional and Administrative News*, the standard collection of legislative history. Mr. Meese explained the purpose of the project as follows:

> To make sure that the President's own understanding of what's in a bill is the same . . . or is given consideration at the time of statutory construction later on by a court, we have now arranged with the West Publishing Company that the presidential statement on the signing of a bill will accompany the legislative history from Congress so that all can be available to the court for future construction of what that statute really means.

Source: Department of Justice. "The Legal Significance of Presidential Signing Statements." Memorandum for Bernard N. Nussbaum, Counsel to the President. November 3, 1993,http://www.usdoj.gov/olc/signing.htm

2. The thesis that emerges from this study is that the George W. Bush administration has very effectively expanded the scope and character of the signing statement not only to address specific provisions of legislation that the White House wishes to nullify, but also in an effort to significantly reposition and strengthen the powers of the presidency relative to the Congress. This tour d' force has been carried out in such a systematic and careful fashion that few in Congress, the media, or the scholarly community are aware that anything has happened at all.

While there certainly were examples in the past of the use of signing statements (Fisher 1997, 132-41; Dellinger 1993), it was Ronald Reagan's attorney general, Edwin Meese III, who was responsible for the development of the signing statement into a significant and commonly used

instrument of executive direct action. Prior to Reagan, such statements were rarely used for the kinds of substantive purposes to which they would be put starting with the Reagan years. Looking back prior to the Reagan administration, Assistant Attorney General Walter Dellinger found some sixteen situations in which thirteen different presidents issued signing statements that addressed what the president considered to be problematic parts of legislation presented for signature (Dellinger 1993). The Reagan administration saw the signing statement as a useful and potentially important tool.

> Signing statements are attractive for two related legal reasons. The first is that they are, in most cases, extremely difficult to challenge unless an administration deliberately makes clear specifically how and in what circumstances it will invoke the terms of the signing statement.

Source: Phillip J. Cooper. "George W. Bush, Edgar Allan Poe, and the Use and Abuse of Presidential Signing Statements. " *Presidential Studies Quarterly* 35 no. 3 (2005): 515-533.

3. For important legislation, however, presidents often prepare signing statements to publicize, explain, or justify their decisions. These statements may praise or criticize the legislation in question, and they are important primarily for their political, not legal significance.

In the 1980s, a significant controversy arose concerning legal cognizance of presidential signing statements. On occasion, presidents would use signing statements to impose their interpretation of a statute. Under President Ronald Reagan, this practice became systematic.

Source: Leonard W. Levy and Louis Fisher. *Encyclopedia of the American Presidency.* New York: Simon & Schuster, 1994. 1372-1373.

4. While the number of provisions challenged or objected to by President Bush has given rise to controversy, it is important to note that the substance of his signing statements do not appear to differ substantively from those issued by either Presidents Reagan or Clinton. As with those Administrations, the majority of the Bush II signing statements make generalized objections to perceived encroachments on executive authority. Moreover, in almost all instances where President Bush has raised a constitutional concern or objection, he has stated that he will construe the provision at issue in a manner that will avoid his concerns. Relatedly, in some statements that raise constitutional objections, President Bush has declared that he would comply with the provision at issue "as a matter of comity." Professor Philip J. Cooper has characterized the constitutional objections raised by President Bush as falling across seventeen categories, ranging from generalized assertions of presidential authority to supervise the

"unitary executive branch" to federalism limits imposed by the Supreme Court in *United States v. Printz*.

Source: T.J. Halstead. "Presidential Signing Statements: Constitutional and Institutional Implications." *CRS Report to Congress* September 22, 2006, http://www.fas.org/sgp/crs/natsec/RL33667.pdf

5. There is no established definition of "signing statement." Signing statements usually take the form of a presidential statement or press release issued in connection with the President's signing of a bill. There is even some disagreement as to the first historical use of a signing statement. Many scholars cite President Andrew Jackson's statement accompanying an appropriations act involving internal improvements as the first signing statement. Other scholars point to a statement made by President James Monroe a month after signing a law regulating the appointment of military officers. Various presidential administrations have used signing statements since the early nineteenth century with a variety of responses by Congress and the courts.

Source: GAO. *Presidential Signing Statements Accompanying the Fiscal Year 2006 Appropriations Acts,* June 18, 2007, http://www.gao.gov/decisions/appro/308603.htm

6. In addition, this statement failed to identify the specific nature of concerns, stating only that the provisions "could inhibit the President's ability to carry out his constitutional obligations to take care that the laws be faithfully executed, to protect national security, to supervise the executive branch, and to execute his authority as Commander in Chief." The nature of these objections, however, is not clarified or substantiated according to T.J. Halstead of the Congressional Research Service. As pointed out by Professor Nicholas Quinn Rosenkranz of Georgetown University's law School, the statement leaves the President's constitutional objections "somewhat theoretical," at best.

Source: Findings of the Subcommittee on Oversight and Investigations in Support of the Full Committee re: Presidential Signing Statements, http://www.fas.org/sgp/congress/2008/signing.pdf; also see GPO Access, Committee on the Judiciary, Senate Hearing 109-1053, *The Use of Presidential Signing Statements*, June 27, 2006 , TEXT | PDF United States. Congress. House. Committee on the Judiciary, *Presidential signing statements under the Bush administration : a threat to checks and balances and the rule of law?* : hearing before the Committee on the Judiciary, House of Representatives, One Hundred Tenth Congress, first session, January 31, 2007. Washington : U.S. G.P.O., http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_house_hearings&docid=f:32844.pdf

### President's Daily Brief

1. CIA classified national security information and analysis sent to the President daily; is

"inherently privileged," according to the CIA, and therefore cannot be publicly disclosed, regardless of age or content.

Source: See "Professor Sues CIA for President's Daily Brief," December 23, 2004, http://www2.gwu.edu/~nsarchiv/pdbnews/index.htm

2. The President's Daily Brief has undergone an equally significant transformation. The CIA's Directorate of Intelligence is still the backbone of the PDB and will remain so, but the PDB now benefits from the participation of analysts across the IC. This has brought more expertise to bear and made it easier to identify analytic disagreements and intelligence gaps.

Source: John D. Negroponte, "Transforming Intelligence -- A Focus on Analysis Intelligence and National Security Alliance," June 07, 2006, http://www.dni.gov/speeches/printer_friendly/20060607_speech_print.htm

**President's Foreign Intelligence Advisory Board**

***See Intelligence Oversight Board***

The President's Foreign Intelligence Advisory Board (PFIAB) provides advice to the President concerning the quality and adequacy of intelligence collection, of analysis and estimates, of counterintelligence, and of other intelligence activities. The PFIAB, through its Intelligence Oversight Board, also advises the President on the legality of foreign intelligence activities. The PFIAB currently has 16 members selected from among distinguished citizens outside the government who are qualified on the basis of achievement, experience, independence, and integrity.

Unique within the government, the PFIAB traditionally has been tasked with providing the President with an independent source of advice on the effectiveness with which the intelligence community is meeting the nation's intelligence needs and the vigor and insight with which the community plans for the future.

Source: The White House. Foreign Intelligence Advisory Board, http://www.whitehouse.gov/administration/eop/piab/

**Primary Censorship**

***See Censorship***

Armed forces censorship performed by personnel of a company, battery, squadron, ship, station, base, or similar unit on the personal communications of persons assigned, attached, or otherwise under the jurisdiction of a unit.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Prior Restraint**

In further arguments [in the *Progressive* case], the government noted that 'prior restraints have been upheld by the courts where the government has demonstrated the need to preserve the secrecy of classified or sensitive information." Examples cited included secrecy restrictions imposed on former CIOA employees, and restraints against a government contractor's communication details about constructing and operating a torpedo.

Source: Alexander DeVolpi et al. *Born Secret: the H-bomb, the Progressive Case and National Security.* New York: Pergamon Press, 1981. 59.

**Prisoner of War Censorship**

***See Censorship***

The censorship of the communications to and from enemy prisoners of war and civilian internees held by the United States Armed Forces.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Privacy**

Judge Thomas Cooley defined as "the right to be left alone."

Source: *Treatise on the Law of Torts* (Its ed., 1879; *Id 29*), Samuel Warren and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* IV no. 5 (1890) http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm, "Context" of W/B article http://faculty.uml.edu/sgallagher/harvard__law_review.htm, and Ellen Alderman and Caroline Kennedy. *The Right to Privacy*. New York: Vintage Books, 1997.

**Privacy Act of 1974 (P.L. 93-579)**

Each agency that maintains a system of records shall . . . upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence."

Source: 5 U.S.C. § 552a (d) (1), "Overview of the Privacy Act of 1974," http://www.usdoj.gov/opcl/1974privacyact-overview.htm and EPIC "The Privacy Act of 1974,"

http://www.epic.org/privacy/1974act/

**Privacy and Civil Liberties Oversight Board (PCLOB)**

1. Recommended by the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), the Privacy and Civil Liberties Oversight Board (PCLOB) was initially established as an agency within the Executive Office of the President (EOP) in 2004. Critics, however, maintained that the board appeared to be a presidential appendage, devoid of the capability to exercise independent judgment and assessment or to provide impartial findings and recommendations. This viewpoint gained acceptance in the 110th Congress when the PCLOB was reconstituted as an independent agency within the executive branch by the Implementing Recommendations of the 9/11 Commission Act (IR9/11CA), signed into law on August 6, 2007.

Source: Harold Relyea, "Privacy and Civil Liberties Oversight Board: New Independent Agency," *CRS Report for Congress* November 26, 2008, RL34385, http://www.fas.org/sgp/crs/misc/RL34385.pdf

2. The Board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. This includes advising on whether adequate guidelines, supervision, and oversight exist to protect these important legal rights of all Americans.

In addition, the Board is specifically charged with responsibility for reviewing the terrorism information sharing practices of executive branch departments and agencies to determine whether guidelines designed to appropriately protect privacy and civil liberties are being followed,

Source: Privacy Board, [See the Wayback Machine, http://web.archive.org/web/20080122053540/http://www.privacyboard.gov/ ]

**Privilege**

1. It is my opinion that various types of rights, or privilege are inextricably tied to control – and sometimes not in a negative way – of information; privilege outlines specialized, controlled access to, and power over, information which can encourage public disclosure, ensure confidentiality, or impose secrecy:

**Types of Privilege**:

- Attorney-Client Privilege

Confidential, open communication between a client and attorney so the attorney is completely informed of all facts in a legal matter.

Source: *Federal Rules of Civil Procedure* at R. 26, http://www.law.cornell.edu/rules/frcp/ and the *Federal Rules of Evidence* at R. 501, http://www.law.cornell.edu/rules/fre/

- Attorney Work Product Doctrine Privilege

Both the attorney and client can assert the work product doctrine privilege. It is not designed to protect client confidences but, rather, to shelter the "mental processes" of the attorney. It is considered an independent source of immunity from discovery. *Fed. R. Civ. P.* 26(b)(1) states that, parties may obtain discovery, regarding any matter, not privileged, ... R. 26(b)(3) defines privilege as prepared in anticipation of litigation or for trial by or for another party or by or for that party's representative.

Source: *Federal Rules of Civil Procedure* at R. 26, http://www.law.cornell.edu/rules/frcp/ and the *Federal Rules of Evidence* at R. 501, http://www.law.cornell.edu/rules/fre/

- Audit Privilege

Also known as *industry self-audit* and *polluter secrecy*, allows companies to evaluate practices and operations to ascertain compliance with all applicable environmental laws and regulations. The public is not involved. If violations occur, the company is encouraged to disclose them to the EPA voluntarily. In return, the EPA will dramatically reduce or waive penalties

Source: Richard Dahl. "Audit-Privilege Laws: The Right to Know Nothing." *Environmental Health Perspectives* 107 no. 10 (1999): http://www.ehponline.org/realfiles/docs/1999/107-10/spheres.html and http://www.epa.gov/compliance/state/authorities.html

- Deliberative Process Privilege

Applies to information generated as a process of Agency discussion and action on a matter. Protects agencies from premature disclosure of proposed policies before they are adopted and to encourage frank discussions on matters of policy between subordinates and superiors. Information of this nature is often referred to as "predecisional" or "deliberate documents."

Source: U.S. Department of Justice. *Freedom of Information Act Guide,* http://www.usdoj.gov/oip/foi-act.htm and *Robert G. Wright v. Federal Bureau of Investigation*, (*Fatal Betrayals* manuscript), http://www.fas.org/sgp/jud/wright050609.pdf

- Executive Privilege

Allows the president and other high officials of the executive branch to keep certain communications private if disclosing those communications would disrupt the functions or

decisionmaking processes of the executive branch. As demonstrated by the Watergate hearings, this privilege does not extend to information germane to a criminal investigation; Presidential claims of a right to preserve the confidentiality of information and documents.

Source: Nolo Press Legal Glossary. http://www.nolo.com/definition.cfm/Term/892DA109-E432-4AD3-B348D9160EA44ECA/alpha/E/; *United States v. Nixon* 418 *U.S.* 683 (1974) ; also see Arthur Schlesinger. *The Imperial Presidency* (New York: Atlantic Monthly, 1973) for a historical discussion of the privilege, and Morton Rosenberg, "Presidential Claims of Executive Privilege: History, Law, Practice and Recent Developments," Updated August 21, 2008 *CRS Report to Congress* RL30319 , http://www.fas.org/sgp/crs/secrecy/RL30319.pdf

- Least Privilege

Principle requiring that each subject be granted the **most** restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://foia.state.gov/REGS/Search.asp

- Privileged Information

Exemption 4 of the Freedom of Information Act has been utilized by some courts as an alternative for protecting non-confidential commercial or financial information. Also related to the Trade Secrets Act.

Source: U.S. Department of Justice. "Exemption 4," Freedom of Information Act Guide, http://www.usdoj.gov/oip/exemption4.htm#privileged

- Self Evaluative Privilege

Designed to protect materials relating to an organization's internal studies for fear that if subjected to the adversary process, many of these studies would never occur or would be severely tempered in the candor.

Source: "The Self Evaluative Privilege as Applied to Self-Regulatory Organizations." Prepared by Faegre & Benson. *The Law Has Its Privileges*. Minneapolis, MN: Minnesota Institute of Legal Education, 1993.

- State Secrets Privilege

A common law evidentiary privilege that allows the government to deny discovery of military secrets. In *United States v. Reynolds*, 345 *U.S.* 1, 97 L. Ed. 727, 73 *S. Ct.* 528 (1953), the Supreme Court defined the process through which the government can claim the state secrets privilege, "which is not to be lightly invoked."

Source: FAS. *Secrecy News* April 21, 2004, http://www.fas.org/sgp/jud/index.html#reynolds and Edward C. Liu, "The State Secrets Privilege and Other Limits on Litigation Involving Classified Information," *CRS Reports for Congress* R40603 May 28, 2009, http://www.fas.org/sgp/crs/secrecy/R40603.pdf

- Petitioners, heirs to the original plaintiffs in Reynolds, are now asking the Supreme Court to review the case and to permit them to argue that they were defrauded by the government. The petitioners were rebuffed by the Court in 2003 when they first sought reconsideration of the 1953 ruling, and their arguments have subsequently been rejected by the lower courts as well. Still, the case raises interesting questions not only about the integrity of the original Reynolds decision, which is a cornerstone of national security law, but also about the judicial system's capacity to acknowledge and correct its errors.

Source: FAS. Secrecy News January 5, 2006, http://www.fas.org/sgp/news/secrecy/2006/01/010506.html; Petition for a Writ of Certiorari in *Herring v. U.S.*, filed at the Supreme Court on December 21, 2005, http://www.fas.org/sgp/jud/herring1205.pdf and Louis Fisher. *In the Name of National Security: Unchecked Presidential Power and the Reynolds Case*. Lawrence: University Press of Kansas, 2006.

- Between the years 1953-1976, the privilege was used 4 times; Since 2001, the States Secret privilege has been invoked 23 times.

Source: Rick Blum. *Secrecy Report Card 2005.* OpenTheGovernment.org. September 2005, http://www.openthegovernment.org/otg/SRC2005.pdf

- Mr. Khaled El-Masri, a German citizen of Lebanese origin alleged that he was kidnapped and tortured under the CIA's "extraordinary rendition" program. The case was dismissed after the CIA invoked the state secrets privilege. In his dismissal of the El-Masri case, Judge T.S. Ellis, III wrote that "To succeed on his claims, El-Masri would have to prove that he was abducted, detained, and subjected to cruel and degrading treatment, all as part of the United States' extraordinary rendition program. As noted above, any answer to the complaint by the defendants risks the disclosure of specific details about the rendition argument."

Source: *Khaled El-Masri v. George Tenent*. Case No. 1:05cv1417, http://www.fas.org/sgp/jud/statesec/elmasri051206.pdf; (*Richard Horn v. Franklin Huddle Jr.*) *Secrecy News* blog: "Sealed V. Sealed: How Courts Confront State Secrets," http://www.fas.org/blog/secrecy/2006/06/sealed_v_sealed_how_courts_con.html

– The states secret privilege was used by the *New York Times* – not a federal entity – in "a motion to dismiss the libel suit brought against it by Steven J. Hatfill, the former Army scientist who said he was erroneously linked by the Times to the 2001 anthrax attacks."

Source. FAS, *Secrecy News* January 22, 2007, http://www.fas.org/blog/secrecy/2007/01/the_state_secrets_doctrine_and.html

– Now, along these same lines, my administration is also confronting challenges to what is known as the "state secrets" privilege. This is a doctrine that allows the government to challenge legal cases involving secret programs. It's been used by many past Presidents -- Republican and Democrat -- for many decades. And while this principle is absolutely necessary in some circumstances to protect national security, I am concerned that it has been over-used. It is also currently the subject of a wide range of lawsuits. So let me lay out some principles here. We must not protect information merely because it reveals the violation of a law or embarrassment to the government. And that's why my administration is nearing completion of a thorough review of this practice.

And we plan to embrace several principles for reform. We will apply a stricter legal test to material that can be protected under the state secrets privilege. We will not assert the privilege in court without first following our own formal process, including review by a Justice Department committee and the personal approval of the Attorney General. And each year we will voluntarily report to Congress when we have invoked the privilege and why because, as I said before, there must be proper oversight over our actions.

Source: Barack Obama, "Remarks by the President on National Security," May 21, 2009, NARA, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-On-National-Security-5-21-09/

A selected list of state secret cases can be found at Federation of American Scientists website: http://www.fas.org/sgp/jud/statesec/index.html; "Shays Looks to Limit State Secrets Privilege," OMB *Watch* June 27, 2006, http://www.ombwatch.org/article/articleview/3481/1/451; Louis Fisher. *In the Name of National Security: Unchecked Presidential Power and the Reynolds Case*. Lawrence: University Press of Kansas, 2006; *Practical Guidelines for Invoking the State Secrets Privilege*, U.S. Army Memorandum for File, April 24, 2001, http://www.fas.org/sgp/jud/statesec/army-ssp.pdf and United States. Congress. Senate. Committee on the Judiciary. *State Secrets Protection Act: Report Together with Minority Views (to accompany S. 2533*) (including cost estimate of the Congressional Budget Office). Washington, D.C.: U.S. G.P.O., 2008, http://purl.access.gpo.gov/GPO/LPS99667, and DOJ. "Attorney General Establishes New State Secrets Policies and Procedures,"September 23, 2009, http://www.justice.gov/opa/pr/2009/September/09-ag-1013.html

- Statutory Privilege

A CIA "conceit referring to the statutory requirement that the DCI must protect intelligence sources and methods. Although this statute is often employed in a self-interested way, it is an obligation of law and not a "privilege" that can be waived."

Source: FAS. *Secrecy News* April 23, 2002, http://www.fas.org/sgp/news/secrecy/2002/04/042302.html

**Privileged Information**

Exemption 4 of the Freedom of Information Act has been utilized by some courts as an alternative for protecting non-confidential commercial or financial information. Also related to The Trade Secrets Act.

Source: U.S. Department of Justice. "Exemption 4," *Freedom of Information Act Guide*, http://www.usdoj.gov/oip/exemption4.htm#privileged

**Privileged Records**

Sec. 8. Withholding of Privileged Records During 12-Year Period. In the period not to exceed 12 years after the conclusion of a Presidency during which section 2204(a) and section 2204(b) of title 44 apply, a former President or the incumbent President may request withholding of any privileged records not already protected from disclosure under section 2204. If the former President or the incumbent President so requests, the Archivist shall not permit access to any such privileged records unless and until the incumbent President advises the Archivist that the former President and the incumbent President agree to authorize access to the records or until so ordered by a final and nonappealable court order.

Source: "Presidential Records Act Executive Order Further Implementation of the Presidential Records Act Executive Order." November 1, 2001, 2001 [See the Wayback Machine, http://tinyurl.com/ycrzvc7 ]

**ProActive Intelligence (PAINT)**

*S*eeks to study the dynamics of complex intelligence targets (inclusive of terrorist organizations) by examining patterns of causal relationships that are indicative of nefarious activity.

Source: DNI, *Data Mining Report*, February 15, 2008, http://www.fas.org/irp/dni/datamining.pdf

**Procedure Words**

To keep voice transmissions as short and clear as possible, radio operators employ procedure words (prowords)—a word or phrase limited to radio telephone procedure, used to facilitate communication by conveying information in a condensed standard form.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Process**

An information management activity: to raise the meaning of information from data to knowledge.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Processing and Exploitation**

(DOD) In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Project Camelot**

***See Minerva Consortia***

Project Camelot has as its main objective an evaluation of the feasibility of developing and implementing a dynamic social systems model to:
a. identify indicators of conditions and trends which, if continued, would probably lead to the outbreak of internal war; b. determine the probable effects of various courses of actions by the indigenous government upon social processes in the indigenous culture; c. maintain information on the conditions referred too in a. and b. above in such a way, including the specifying of dynamic interrelationships among classes of information and the societal elements represented thereby…

Source: (DoD) "Document Number 2," In Irving Louis Horowitz (ed.) *The Rise and Fall of Project Camelot* (Cambridge: MIT Press); Johan Galtung , "After Camelot," Scientific Colonialism," *Transition* no.30 (April-May, 1967): 11-15; Joseph G. Jorgensen, "On Ethics and Anthropology," *Current Anthropology*, 12 no.3 (1971): 321-334; Joy Rohde, Counterinsurgency on Contract: Project Camelot, Social Science, and American National Security in the Cold War Miller Center for Public Affairs, May 10, 2007,

http://webstorage1.mcpa.virginia.edu/library/mc/apd/rohde.pdf; and Kalman H. Silver, "American Academic Ethics and Social Research Abroad: The Lesson of Project Camelot," *Proceedings and Papers: The New Intelligence Requirements* (Nov., 1965): 215-236.

**Propaganda**

***See Bureau of International Information Programs, Counter-Information Team, Information Exploitation, Public Diplomacy, Smith-Mundt Act***

1. Ellul suggests that information and propaganda are indistinguishable in a technological society. [53]

Propaganda is defined as a form of communication that draws upon elements of information and persuasion, and appears to be a form of informative communication, and used to promote institutional objectives that are not necessarily in the best interest of the audience. There are several specific types of propaganda:

**Black or Covert Propaganda**: false sources are given, accompanied by lies, fabrications and deceptions; **Direct Propaganda** must be preceded by propaganda that is sociological in character, slow, general, seeking to create a climate, an atmosphere of favorable preliminary attitudes; **Gray Propaganda**: a source may or may not be correctly identified, and the accuracy of the information is uncertain; often used to embarrass an enemy or competitor; **White or Overt Propaganda**: the source is correctly identified and communicates accurate information; attempts to build credibility.

Source: Jacques Ellul. *Propaganda: The Formation of Men's Attitudes*. New York: Vintage Books, 1973; Victoria O'Donnell, and Garth S. Jowett. "Propaganda as a Form of Communication," *Propaganda: A Pluralistic Perspective*, Ed. Ted J. Smith III. New York: Praeger, 1989. 49-62; Nicholas J. Cull, David Culbert, and David Welch, *Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present*, Santa Barbara, CA: ABC-CLIO, 2003, and Noam Chomsky, *Necessary Illusions: Thought Control in Democratic Societies*, Boston, MA : South End Press, 1989.

[53] It's possible Jacques Ellul based his famous maxim on testimony from select members of the ASNE [American Society of Newspaper Editors] during the *United States Information and Educational Exchange Act of 1947* hearings, [H.R 3342, Smith-Mundt hearing; May 13-14, 16-17, 20, 1947, 80th Congress, First Session. Y 4.F76/1:In3]. The hearings are truly remarkable in their discussion of the U.S. government's role in creating news and "information programs" for international audiences. For example, Mr. McKelway (102) of ASNE states "…let us frankly recognize the Government's program as an experiment in propaganda, and not to confuse that program with the dissemination of untainted news." There are many discussions in these hearings which mirror debates over DoD's video news releases and subsequent GAO investigations of fake news.

2. DOD and NATO terms; Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly.

**Black Propaganda** – Propaganda that purports to emanate from a source other than the true one. See FM 33-1-1.
**Grey Propaganda** – Propaganda that does not specifically identify any source. See FM 33-1-1.
**White Propaganda** – Propaganda disseminated and acknowledged by the sponsor or by an accredited agency thereof. See FM 3-05.30.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

3. Black propaganda and disinformation are virtually indistinguishable. Both refer to the spreading of false information in order to influence people's opinions or actions. Disinformation is a special type of black propaganda which hinges on absolute secrecy and which is usually supported by false documents.

Source: Victor Marchetti, and John D. Marks. *The CIA and the Cult of Intelligence.* New York: Knopf, 1974. 165 and Nicholas J. Cull, David Culbert, and David Welch, *Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present*, Santa Barbara, CA: ABC-CLIO, 2003.

4. The division between the two [black and white propaganda] was recognized during the recent war; the Office of War Information (OWI) was restricted to white, and the Office of Strategic Services (OSS) to black. Over and above them was Psychological Warfare, an armed services organization, but this exercised only the loosest supervision, and where black propaganda was concerned, issued very few if any written orders to field operatives. In the very nature of the case, black had to be kept in a position where it could be honestly disavowed at any time; otherwise public officials and even some military men, objecting to the essential deceit involved in any black operation, might cripple the enterprise.

Among the most important kinds of black propaganda is the planted bit of gossip or rumor.

Becker, Howard. "The Nature and Consequences of Black Propaganda." *American Sociological Review* 14 no. 2 (April 1949): 221-235, and William E. Daugherty. *A Psychological Warfare Casebook.* Baltimore Published for Operations Research Office. Baltimore, MD: Johns Hopkins Press 1958. 221-222.

5. SEC. 821. No part of any funds appropriated in this or any other Act shall be used by an agency of the executive branch, other than for normal and recognized executive-legislative

relationships, for publicity or propaganda purposes, and for the preparation, distribution or use of any kit, pamphlet, booklet, publication, radio, television or film presentation designed to support or defeat legislation pending before the Congress, except in presentation to the Congress itself.

Source: "Making appropriations for the Departments of Transportation, Treasury, and Housing and Urban Development, the Judiciary, District of Columbia, and independent agencies for the fiscal year ending September 30, 2006, and for other purposes. " 109 P.L. 115; 119 Stat. 2396; 2005 Enacted H.R. 3058; 109 Enacted H.R. 3058. November 30, 2005, http://www.gpoaccess.gov/plaws/

**Former Soviet Union IC definitions of propaganda:**

White *belaya* subversive imperialist form of propaganda ideological sabotage. the acuteness of these operations depends on the nature of relations with the country against which they are carried out.

Grey *seraya* subversive imperialist form of propaganda carried out by NGOs, including anti-Soviet émigré centres and private individuals, usually financed by capitalist countries, who are able to "camouflage their subversive activities and deny involvement."

Black *chornaya* subversive imperialist form of propaganda carried out by the enemy in the name of legendary underground groups and opposition elements in socialist countries. The enemy's involvement is carefully concealed. Examples: dropping leaflets and newspapers onto the territory of other countries as though they had been issued there by "underground organizations," (political personalities or citizens in socialist countries) the spreading of false rumours and gossip, radio propaganda, alleged to be broadcast from "underground radio stations"

Source: Vasily Mitrokhin, ed. *KGB Lexicon: The Soviet Intelligence's Officer's Handbook*. London: Frank Cass, 2002.

**Proprietary Information**

1. Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specification; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

2. Proprietary information is information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or impair the government's interest in compliance with program effectiveness.

Source: Centers for Disease Control. "Sensitive But Unclassified Information." February 2006, http://www.fas.org/sgp/othergov/cD.C.-sbu-2006.html

**Proprietary Information Involved (PROPIN)**
***See Classification Markings / Control Markings***

**Proscribed Information**
Proscribed Information is: a. Top Secret information; b. Communication Security (COMSEC) information, except classified keys used to operate secure telephone units (STU IIIs); c. Restricted Data as defined in the U.S. Atomic Energy Act of 1954, as amended; d. Special Access Program (SAP) information; or e. Sensitive Compartmented Information (SCI).

Source: DoD. *National Industrial Security Program Operating Manual* (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

**Protect as Restricted Data**
A handling method for computer-generated numerical data or related information, which is not readily recognized as classified or unclassified because of the high output and low density of potentially classified data. (Note: This information is designated as "Protect as Restricted Data" because it has not had a classification review and must be protected under a different set of security rules."

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

**Protected Critical Infrastructure Information**
Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency

study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in Sec. 29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

Source: Department of Homeland Security. "Protected Critical Infrastructure Information." 6 CFR 29.2, http://www.gpoaccess.gov/cfr/index.html

**Protected Document**

(1) Protected document.--The term ``protected document'' means any record--
(A) for which the Secretary of Defense has issued a certification, as described in subsection (d), stating that disclosure of that record would endanger citizens of the United States, members of the United States Armed Forces, or employees of the United States Government deployed outside the United States; and….

Source: H.R.111-298 Conference Report on H.R.2892, Department of Homeland Security Appropriations Act, 2010, http://www.fas.org/sgp/congress/2009/protected.html and

2. On October 28, 2009, the President signed into law the Department of Homeland Security Appropriations Act, 2010. Section 565 of that Act vests the Secretary with authority to issue a certification with respect to certain photographic records. If such a certification is issued, the covered records are not subject to disclosure under FOIA.

Source: *United States Department of Defense v. American Civil Liberties Union*
http://www.scotusblog.com/wp/wp-content/uploads/2009/11/photos-US-supp-brief-11-13-09.pdf

**Pseudo-Classification**

***See Classification Markings / Control Markings***

Not long ago, in the closing days of January, *GCN Update*, the online, electronic news service of Government Computer News, reported that 'dozens of classified Homeland Security Department documents" had been accidentally made available on a public Internet site for several days due to an apparent security glitch at the Department of Energy. Describing the contents of the materials and reactions to the breach, the account stated that the "documents were marked 'for official use only,' the lowest secret-level classification." The documents, of course, were not security classified, because the marking cited is not authorized by E.O 12958. Interestingly, however, in view of the fact that this misrepresentation appeared in a story to which three reporters contributed, perhaps it reflects, to some extent, the current state of confusion about the origin and status of new information control markings which have appeared of late.

Early indications are that very little of the attention to detail that attends the security classification program is to be found in other information control marking activities. *Key terms often lack definition* [emphasis added]. Vagueness exists regarding who is authorized to applying markings, for what reasons, and for how long. Uncertainty prevails concerning who is authorized to remove markings and for what reasons.

Source: Harold C. Relyea. "Emerging Threats and Pseudo-Classification." Statement before the House Government Reform Subcommittee on National Security, Emerging Threats, and International Relations. March 2, 2005. 9, 19, http://www.fas.org/sgp/congress/2005/030205overclass.html and GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information,* GAO-06-385, March 2006, http://www.gao.gov/new.items/d06385.pdf

**PSYOP**

The earliest recorded use of the "psychological operations" occurred early in 1945 when Captain (later Rear Admiral) Ellis M. Zacharias, U.S. Navy, employed the term in an operation plan designed to hasten the surrender of Japan. Without any description or explanation the term was used in the context "All psychological operations will be coordinated both as to times and trends in order to avoid reduction of effectiveness of this main operation." The next use of the term was in 1951, when the Truman Administration renamed an interagency strategy committee giving it the title Psychological Operations Coordinating Committee. Although the Department of the Army made the change in 1971, it was not until the 1960s that psychological operations came to supplant psychological warfare as the all-inclusive term in common use.

Source: William E. Daugherty. "Origin of psyop terminology." In Ronald De McLaurin, et al (Ed.) The *Art and Science of Psychological Operations: Case Studies of Military Application*. volume 1, Department of the Army, American Institutes for Research, 1976.

**Psychological Operations (PSYOPS)**

***See Information Operations, Information Operations Roadmap, Overt Peacetime, Perception Management, Propaganda, Psychological Operations Program, Public Diplomacy***

1. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/; Joint Publication 3-53. *Doctrine for Joint Psychological Operations*. September 5, 2003, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53.pdf

and Clay Wilson, "Information Operations and Cyberwar: Capabilities and Related Policy Issues." CRS Report to Congress Updated September 14, 2006, http://www.fas.org/sgp/crs/natsec/RL31787.pdf

2. There are three categories of military PSYOP: strategic, operational, and tactical. Strategic PSYOP are international information activities conducted by US Government (USG) agencies to influence foreign attitudes, perceptions, and behavior in favor of US goals and objectives during peacetime and in times of conflict.

Operational PSYOP are conducted across the range of military operations, including during peacetime, in a defined operational area to promote the effectiveness of the joint force commander's (JFC's) campaigns and strategies.

Tactical PSYOP are conducted in the area assigned a tactical commander across the range of military operations to support the tactical mission against opposing forces.

Source: Joint Publication 3-53. *Doctrine for Joint Psychological Operations*. September 5, 2003, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53.pdf

3. (U) PSYOP enhancements outlined in this report, and clarification of respective responsibilities and tasks associated with PSYOP, DoD support to public diplomacy and public affairs, will enhance DoD's ability to aggressively conduct IO and to do so fully consistent with broader national security objectives. (p. 6)

Future operations require that PSYOP capabilities be improved to enable PSYOP forces to rapidly generate and disseminate audience specific, commercial-quality products into denied areas, and that these products focus on aggressive behavior modification of adversaries at the operational and tactical level of war. The likelihood that PSYOP messages will be replayed to a much broader audience, including the American public, requires that specific boundaries be established for PSYOP. In particular:

*(U) PSYOP should focus on support to military endeavors (Exercises, deployments and operations) in a non-permissive or semi-permissive environments (i.e., when adversaries are part of the equation).*

*(U) DoD should collaborate with other agencies for U.S. Government public diplomacy programs and information objectives. PSYOP forces and capabilities can be employed in support of public diplomacy (e.g., as part of approved theater security guidelines).*

*(U) DoD Public Affairs should be more proactive in support of U.S. Government Public Diplomacy objectives to include a broader set of foreign media audiences.* (p.15-16)

Source: National Security Archive. "Rumsfeld's Roadmap to Propaganda: Information Operations Roadmap." January 26, 2006, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/

4. PSYOP is often confused with propaganda, which is practiced by many of our adversaries, and in some cases, by selected U.S. agencies and politicians. Propaganda has connotations of deception and distortion. Propaganda has no rules and can be a mixture of the truth, incorrectly attributed truth (sometimes referred to as gray propaganda), or pure fiction, purposely misattributed (black propaganda or covert propaganda). U.S. DoD PSYOP, on the other hand, are actions taken to influence the emotions, attitudes and ultimately the behavior of a target audience. The intent is to influence target audiences in ways that support USG national policy objectives at the strategic, operational and tactical levels. Additionally, DoD PSYOP programs are always based on truth in order to maintain local and regional credibility equal to or greater than that of public affairs activities and local journalists. In many instances, PSYOP products and activities (newspapers, radio broadcasts, leaflets, hand bills and face-to-face communication) become the primary source of trusted information within an area of conflict or disaster. Another definition is provided in the United States Special Operations Forces Posture Statement which describes PSYOP as "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and, ultimately, the behavior of foreign government organizations, groups and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives."

Source: Col. Brad Ward. "Strategic Influence Operations: The Information Connection." U.S. Army War College. April, 2003, http://www.fas.org/irp/eprint/ward.pdf and David Mugg, *Satan vs. Satan: The Use of Black PSYOP to Regain the Tactical Initiative in the Counterinsurgency Fight* ADA471500, http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA471500

**Psychological Operations Assessment Team**

A small, tailored team (approximately 4 to 12 personnel) that consists of PSYOP planners and product distribution/dissemination and logistics specialists. The team is deployed to theater at the request of the combatant commander to assess the situation, develop PSYOP objectives and recommend the appropriate level of support to accomplish the mission.

Source: DoD. *Psychological Operations,* FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

**Psychological Operations Development Center**

A regional psychological operations unit that designs informational products and programs and makes recommendations to the joint force commander through the joint targeting coordination board for other joint forces to conduct psychological actions in support of military and national objectives. The psychological operations development center is the central core of a psychological operations task force. It consists of a target audience analysis detachment, a plans and programs detachment, and a test and evaluation detachment.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Public Affairs**
Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Public Affairs Ground Rules**
***See Public Affairs***
Conditions established by a military command to govern the conduct of news gathering and the release and/or use of specified information during an operation or during a specific period of time.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Public Affairs Guidance (PAG)**
Normally, a package of information to support the public discussion of defense issues and operations. Such guidance can range from a telephonic response to a specific question to a more comprehensive package. Included could be an approved public affairs policy, contingency statements, answers to anticipated media questions, and community relations guidance. The public affairs guidance also addresses the method(s), timing, location, and other details governing the release of information to the public. Public affairs guidance is approved by the Assistant to the Secretary of Defense for Public Affairs.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Public Diplomacy**

***See Disinformation, Bureau of International Information Programs, Counter-Information Team, Information Operations Roadmap, Propaganda***

1. Through the use of modern instruments and techniques of communication it is possible today to reach large or influential segments of national populations – to inform them, to influence their attitudes, and at times perhaps even motivate them to a particular course of action. These groups, in turn, are capable of exerting noticeable, even decisive, pressures on their governments.

Source: United States. Congress. House. Committee on Foreign Affairs. *Ideological operations and foreign policy. Report no. 2 on Winning the cold war: the U.S.ideological offensive*, by the Subcommittee on International Organizations and Movements of the Committee on Foreign Affairs, House of Representatives, pursuant to H. Res. 55, a resolution authorizing the Committee on Foreign Affairs to conduct thorough studies and investigations of all matters coming within the jurisdiction of the Committee. Washington, D.C.: U.S. GPO, 1964.

2. Those overt international public information activities of the United States Government designed to promote United States foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers, and by broadening the dialogue between American citizens and institutions and their counterparts abroad.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/; also see Reagan NSDD 77, January 15, 198.

3. Engaging, informing, and influencing key international audiences) is practiced in harmony with public affairs (outreach to Americans) and traditional diplomacy to advance U.S. interests and security and to provide the moral basis for U.S. leadership in the world.

Source: U.S. Department of State. "Under Secretary for Public Diplomacy and Public Affairs." http://www.state.gov/r/; also see William P. Kiehl, "Can Humpty Dumpty Be Saved?" *American Diplomacy* 8 no. 4 (2002), http://www.publicdiplomacy.org/98.htm, Alvin A. Snyder, *Warriors of Disinformation: American Propaganda, Soviet Lies, and the Winning of the Cold War, An Insider's Account* (New York: Arcade Pub., 1995), Nicholas J. Cull, David Culbert, and David Welch, *Propaganda and Mass Persuasion: A Historical Encyclopedia, 1500 to the Present*, (Santa Barbara, CA: ABC-CLIO, 2003), Geoffrey Cowan and Nicholas J. Cull. (eds.), *Public Diplomacy in a Changing World*, (Thousand Oaks, CA: Sage, 2008), and Laura Alexandre, "In the service of the state: public diplomacy, government media and Ronald Reagan." *Media, Culture & Society* 9 no.1 (1987): 29-46.

Note: See "Pentagon Closes Office Accused of Issuing Propaganda Under Bush" (Thom Shanker, *New York Times* April 15, 2009, http://www.nytimes.com/2009/04/16/us/politics/16policy.html)

**Public Domain**
Classified information that has made its way into the public domain, either by leak or unauthorized disclosure.

Source: U.S. Department of Justice. *Freedom of Information Act Guide*, http://www.usdoj.gov/oip/exemption1.htm#public

**Public Information**
Information of a military nature, the dissemination of which through public news media is not inconsistent with security, and the release of which is considered desirable or nonobjectionable to the responsible releasing agency

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Public Information Environment**
All individuals, organizations or systems that collect, process and disseminate information for public consumption. (AFDD 2-5)

Source: U.S. Air Force. Public Affairs Operations. Air Force Doctrine Document 2-5.3, June 24, 2005, [See Wayback Machine, http://web.archive.org/web/20061007174450/http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5.3/afdd2-5.3.pdf ]

**Public Interest Declassification Board**
(b) PURPOSES- The purposes of the Board are as follows:

(1) To advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board considers appropriate on the systematic, thorough, coordinated, and comprehensive identification, collection, review for declassification, and release to Congress, interested agencies, and the public of declassified records and materials (including donated historical materials) that are of archival value, including records and materials of extraordinary public interest.

(2) To promote the fullest possible public access to a thorough, accurate, and reliable documentary record of significant United States national security decisions and significant United States national security activities in order to--

(A) support the oversight and legislative functions of Congress;

(B) support the policymaking role of the executive branch;

(C) respond to the interest of the public in national security matters; and

(D) promote reliable historical analysis and new avenues of historical study in national security matters.

Source: "Public Interest Declassification Board." 108 P.L. 458; 118 Stat. 3638; 2004 Enacted S. 2845; 108 Enacted S. 2845.FAS, http://www.fas.org/sgp/congress/2005/pida.html

**Publicly Available Information**
Information that is generally accessible to the interested public in any form and, therefore, not subject to the EAR (See part 732 of the Export Administration Rules (EAR).

Source: Commerce and Foreign Trade. 15 CFR 772.1, http://www.gpoaccess.gov/cfr/index.html

**Purging**
Rendering stored information unrecoverable.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

---

**~ Q ~**

**Quantico Circuit**
Named for the FBI's Academy on the United States Marine Corps Base at Quantico, Virginia, the warrantless surveillance program gives the U.S. government direct high-speed access to wireless carriers and hence voice calls/messages and data packets.

Source: "New Telecom Whistleblower Describes Open Surveillance Gateway," Electronic Frontier Foundation *EFFector* 21, no.8 March 7, 2008, http://w2.eff.org/effector/21/16.php and Kevin Poulson, "Whistle-Blower: Feds Have a Backdoor Into Wireless Carrier -- Congress Reacts," March 6, 2008, http://blog.wired.com/27bstroke6/2008/03/whistleblower-f.html

**Quasi Government**
***See In-Q-Tel***
The quasi government, virtually by its name alone and the intentional blurring of the governmental and private sectors, is not easily defined. In general, the term is used in two ways: to refer to entities that have some legal relation or association, however tenuous, to the federal government; or to the terrain that putatively exists between the governmental and private sectors. For the most part, this report will use the term quasi government in the former context, referring to entities with some legal relationship to the federal government. The one common characteristic to this melange of entities in the quasi government is that they are *not* agencies of the United

States as that term is defined in Title 5 of the *U.S. Code*.

Source: Kevin R. Kosar, "The Quasi Government: Hybrid Organizations with Both Government and Private Sector Legal Characteristics," *CRS Report to Congress* Updated February 13, 2007, http://www.fas.org/sgp/crs/misc/RL30533.pdf

---

**~ R ~**

**Real-time Analytical Intelligence Database (RAID) and Hashkeeper**
***See National Media Exploitation Center***
RAID is a relational database used to record key pieces of information and to quickly identify links among people, places, businesses, financial accounts, telephone numbers, and other investigative information examined by our analysts.

HashKeeper is a software application that quickly eliminates known operating system files and focuses on electronic files created by the user/subject of the investigation

Source: DOJ, National Drug Intelligence Center, "Document and Media Exploitation," http://www.usdoj.gov/ndic/domex/domex.pdf

**Rapid Reaction Media Team (RRMT)**
RRMT will serve as a "quick start bridge" between Saddam Hussein's state-controlled media network and a longer "Iraqi Free Media" network in a post-Saddam era. The major elements of the RRMT are
2.1 USG media experts team
2.2UK experts
2.3 Handpicked Iraqi media experts

Source: Joyce Battle, "Pentagon 'Rapid Reaction Media Team' for Iraq" Electronic Briefing Book, National Security Archive, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB219/index.htm, includes documents obtained via FOIA (as cited above).

**Raw Intelligence (RI)**
Information that has been obtained from generally reliable sources; however, it is not necessarily corroborated. It is deemed valid not only because of the sources but also because it coincides with other known information. Raw intelligence usually is time sensitive and its value is perishable in a relatively short period.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404

**Real Time**

Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. See FM

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004. http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Reclassification**

***See Retroactive Secrecy***

1. Restoration of classification to information previously classified as National Security Information and then declassified.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. The CIA and other federal agencies have secretly reclassified over 55,000 pages of records taken from the open shelves at the National Archives and Records Administration (NARA), according to a report published today on the World Wide Web by the National Security Archive at George Washington University. Matthew Aid, author of the report and a visiting fellow at the Archive, discovered this secret program through his wide-ranging research in intelligence, military, and diplomatic records at NARA and found that the CIA and military agencies have reviewed millions of pages at an unknown cost to taxpayers in order to sequester documents from collections that had been open for years.

To justify their reclassification program, officials at CIA and military agencies have argued that during the implementation of Executive Order 12958, President Clinton's program for bulk declassification of historical federal records, many sensitive intelligence-related documents that remained classified were inadvertently released at NARA, especially in State Department files. Even though researchers had been combing through and copying documents from those collections for years, CIA and other agencies compelled NARA to grant them access to the open files so they could reclassify documents. While this reclassification activity began late in the 1990s, its scope widened during the Bush administration, and it is scheduled to continue until 2007. The CIA has ignored arguments from NARA officials that some of the impounded documents have already been published.

Source: Aid, Matthew M. (ed.). *Declassification in Reverse: The U.S. Intelligence Community's Secret Historical Document Reclassification Program.* National Security Archive, February 21, 2006, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/

3. The audit also found that in attempting to recover records that still contained classified information, there were a significant number of instances when records that were clearly inappropriate for continued classification were withdrawn from public access. We concluded that 24 percent of the sampled records fell into this category, and an additional 12 percent were questionable. In one re-review effort, the Central Intelligence Agency (CIA) withdrew a considerable number of purely unclassified records in order to obfuscate the classified equity that the agency was intent on protecting. Included in the inappropriate category above, at least 12 percent of the records sampled had apparently been properly declassified, but were later improperly reclassified.

Source: Information Security Oversight Office (ISOO). Audit of the Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes. April 26, 2006. http://www.archives.gov/isoo/reports/2006-audit-report.html

**Record**

1. The term "record", when used in connection with the proceedings of a court-martial, means:

(A) an official written transcript, written summary, or other writing relating to the proceedings; or

(B) an official audiotape, videotape, or similar material from which sound, or sound and visual images, depicting the proceedings may be reproduced.

Source: "Armed Forces." 10 U.S.C. 47 § 801, http://www.gpoaccess.gov/U.S.C.ode/

2. In the Privacy Act of 1974, a record is "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

Source: 5 U.S.C. 552a(a)(4). The Privacy Act of 1974 http://www.usdoj.gov/opcl/privstat.htm and EPIC, http://www.epic.org/privacy/1974act/ [supplied by Robert Gellman].

3. A record means any item of information about an individual that includes an individual identifier and can include as little as one descriptive item about an individual.

Source: "Office of Management and Budget Privacy Act Implementation Guidelines and Responsibilities" (July 9, 1975), http://www.defenselink.mil/privacy/1975OMB_PAGuide/75JULY09.pdf [supplied by Robert Gellman].

### Record Group

NARA arranges its holdings according to the archival principle of *provenance*. This principle provides that records be

- attributed to the agency that created or maintained them and
- arranged thereunder as they were filed when in active use.

In the National Archives, application of the principle of provenance takes the form of numbered record groups, with each record group comprising the records of a major government entity, usually a bureau or an independent agency. For example, *National Archives Record Group 4* is *Records of the U.S. Food Administration*.

Source: National Archives and Records Administration (NARA). "The Record Group Concept." Excerpted from: *Guide to Federal Records in the National Archives of the United States.* Compiled by Robert B. Matchette et al. Washington, D.C.: National Archives and Records Administration, 1995, http://www.archives.gov/research/guide-fed-records/index numeric/concept.html and Record Group Clusters Contents and Locations. http://www.archives.gov/research/alic/tools/record-group-clusters.html

### Record Information

All forms (e.g., narrative, graphic, data, computer memory) of information registered in either temporary or permanent form so that it can be retrieved, reproduced, or preserved.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

### Records

1. Records of an agency and Presidential papers or Presidential records, as those terms are defined in Title 44 *United State Code*, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

2. The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the

information are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Source: National Institute of Standards and Technology (NIST) Special Publication 800-53, "Information Security." http://csrc.nist.gov/publications/PubsSPs.html

3. Includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them (44 *U.S.C* 3301).

Source: NARA. "Federal Records, General." 36 CFR 1220, http://www.gpoaccess.gov/CFR/index.html

## Types of Records

- Abandoned Records

Records that support a program that no longer exist, or can be identified, regardless of media. Also known as "orphaned records". Records deserted by federal and contractor employees. This usually occurs when personnel relocate, transfer, or terminate. Abandoning records is a common practice throughout DOE.

Source: DOE. Chief Information Officer. "Records Management Definitions." http://cio.energy.gov/rmdefinitions.pdf

- Accessioned Records

Records of permanent historical value in the legal custody of NARA (National Archives and Records Administration).

Source: "Classified National Security Information." 32 CFR 2001, http://www.gpoaccess.gov/CFR/index.html.

- Administrative Records

Records relating to budget, personnel, supply, and similar housekeeping, or facilitative, functions common to most agencies, in contrast to program records.

Source: DOE. Chief Information Officer. "Records Management Definitions."

http://cio.energy.gov/rmdefinitions.pdf

- Agency Records

A record in the possession and control of the Nuclear Regulatory Commission (NRC) that is associated with Government business. Agency record does not include records such as:

(1) Publicly-available books, periodicals, or other publications that are owned or copyrighted by non-Federal sources; (2) Records solely in the possession and control of NRC contractors; (3) Personal records in possession of NRC personnel that have not been circulated, were not required to be created or retained by the NRC, and can be retained or discarded at the author's sole discretion, or records of a personal nature that are not associated with any Government business; or (4) Non-substantive information in logs or schedule books of the Chairman or Commissioners, uncirculated except for typing or recording purposes.

Source: Nuclear Regulatory Commission (NRC). 10 CFR § 9.13 "Definitions." http://www.gpoaccess.gov/CFR/index.html

- Consumer Records

Consumer reports pertaining to the employee under the Fair Credit Reporting Act.

Source: "Commerce and Trade." 15 U.S.C. 1681a, http://www.gpoaccess.gov/U.S.C.ode/

- Financial Records

Maintained by a financial institution as defined in 31 *U.S.C* 5312(a) or by a holding company as defined in section 1101(6) of The Right to Financial Privacy Act of 1978 (12 U.S.C 3401): As part of all investigations and reinvestigations, agencies may request the Department of the Treasury to search currency transaction databases for international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under $10,000 that are reported as possible money laundering violations, and records of foreign travel.

Source: "Money and Finance." 31 U.S.C. 5312(a), section 1101(6) of The Right to Financial Privacy Act of 1978 (12 U.S.C. 3401), http://www.gpoaccess.gov/U.S.C.ode/

- Newly Discovered Records

Records that were inadvertently not reviewed prior to the effective date of automatic declassification because the agency declassification authority was unaware of their existence.

Source: "Classified National Security Information." 32 CFR 2001, http://www.gpoaccess.gov/CFR/index.html.

- Official Record

Section 3 (c) of provides that "Save as otherwise required by statute, matters of official record shall in accordance with published rule be made available to persons properly and directly concerned except information held confidential for good cause found." The introductory saving clause is intended to preserve existing statutory requirements for confidential treatment of certain materials, such as income tax returns.

Each agency should publish in the *Federal Register*, under 3 (a) (1), a rule listing the types of official records in its files, classifying them in terms of whether or not they are confidential in character, stating the manner in which information is available (as by inspection or sale of photostatic copies), the method of applying for information, and by what officials the application will be determined.

The term "official record" is difficult of definition. In general, it may be stated that matters of official record will include (a) applications, registrations, petitions, reports and returns filed by members of the public with the agency pursuant to statute or the agency's rules, and (b) all documents embodying agency actions, such as orders, rules and licenses. In formal proceedings, the pleadings, transcripts of testimony, exhibits, and all documents received in evidence or made a part of the record are "matters of official record."

Section 3 (c) does not purport to define "official record." Each agency must examine its functions and the substantive statutes under which it operates to determine which of its materials are to be treated as matters of official record for the purposes of the section. Indicative of the types of records which are considered official records by Congress are maps, plats, or diagrams in the custody of the Secretary of the Interior (5 U.S.C. 488), [25] records, books or papers in the General Land Office (28 U.S.C. 672), and registration statements filed with the Securities and Exchange Commission under the Securities Act (15 U.S.C. 77f).

Source: *Attorney General's Manual on the Administrative Procedure Act*. Prepared by the United States Department of Justice Tom C. Clark, Attorney General, 1947, http://www.law.fsu.edu/library/admin/1947cover.html

- Permanent Records

Permanent Records" means any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States. Permanent records include all records accessioned by NARA into the National Archives of the United States and later increments of the same records, and those for which the disposition is permanent on SF 115s, Request for Records Disposition Authority, approved by NARA on or after May 14, 1973.

Source: "Classified National Security Information." 32 CFR 2001, http://www.gpoaccess.gov/CFR/index.html.

- Presidential Record

The Presidential Records Act of 1978 defines a presidential record as:

> …documentary materials, or any reasonably segregable portion thereof, created or received by the President, his immediate staff, or a unit or individual of the Executive Office of the President whose function is to advise and assist the President, in the course of conducting activities which relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President.

- Public Records

Each state has a public records law that specifically defines and outlines access to public information. Medical records, adoption records and some types of criminal records are considered exempt from public access due to privacy concerns. Arrests and search warrants, indictments, criminal summons, and non-testimonial identification orders are public unless sealed by court order.

- Records Having Permanent Historical Value

Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with Title 44 *United State Code*.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information."
http://www.archives.gov/federal-register/executive-orders/2003.html

- Rights-and-Interests Records

That type of vital records essential to protecting the rights and interests of an organization and of the individuals directly affected by its activities.

Source: DOE. Chief Information Officer. "Records Management Definitions."
http://cio.energy.gov/rmdefinitions.pdf

- Suspense Files

Files arranged chronologically to remind officials of actions to be completed by a specific date. Also called followup files or tickler files.

Source: DOE. Chief Information Officer. "Records Management Definitions."

http://cio.energy.gov/rmdefinitions.pdf

- Temporary Records

Any records which have been determined by the Archivist of the United States to have insufficient value (on the basis of current standards) to warrant its preservation by the National Archives and Records Administration. This determination may take the form of:
(a) A series of records designated as disposable in an agency records disposition schedule approved by NARA (Standard Form 115, Request for Records Disposition Authority); or
(b) A series of records designated as disposable in a General Records Schedule. Unscheduled records are records the final disposition of which has not been approved by NARA.

Source: NARA. "General Records Management Definitions."
http://www.archives.gov/midatlantic/agencies/records-mgmt/definitions.html

- Textual Files

The term usually applied to manuscript and typescript paper records, as distinct from electronic, audiovisual, cartographic, remote-sensing imagery, architectural, and engineering records.

Source: DOE. Chief Information Officer. "Records Management Definitions."
http://cio.energy.gov/rmdefinitions.pdf

- Unscheduled records

Are those that have not been included on a Standard Form 115, Request for Records Disposition Authority, approved by NARA; those described but not authorized for disposal on an SF 115 approved prior to May 14, 1973; and those described on an SF 115 but not approved by NARA (withdrawn, canceled, or disapproved).

Source: NARA. "General Records Management Definitions."
http://www.archives.gov/midatlantic/agencies/records-mgmt/definitions.html

- Vital Records

Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the rights and interests of that organization and of the individuals directly affected by its activities. Sometimes called essential records. Include both emergency-operating and rights-and-interests records. Vital records considerations are part of an agency's records disaster prevention and recovery program.

Source: DOE. Chief Information Officer. "Records Management Definitions."

http://cio.energy.gov/rmdefinitions.pdf

**Recordkeeping System**
A manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

Source: NARA. "Federal Records, General." 36 CFR 1220.
http://www.gpoaccess.gov/CFR/index.html

**Records Management**
1. Planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended.
http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2

2. Basic records management terms are defined in 36 CFR 1220.14. Terms such as database, database management system, electronic mail system, electronic record, and so on.

**Red**
***See Black***
In an information processing context, denotes encrypted/classified data, text, equipment, processes, systems or installations associated with information that requires emanations security protection. For example, wiring that carries unencrypted classified information either exclusively or mixed with unclassified is termed "red."

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003. , June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Redaction**
1. The removal of exempted information from copies of a document.

Agencies are encouraged but are not required to redact documents that contain information that is exempt from automatic declassification under section 3.3 of the Order, especially if the information that must remain classified comprises a relatively small portion of the document.

Source: "Classified National Security Information." 32 CFR 2001.
http://www.gpoaccess.gov/CFR/index.html.

2. Redaction means a sanitization technique that involves removal (editing out) of exempted information from a document.

Source: ISOO. "Classified National Security Information."*Federal Register* November 16, 1999,
http://www.fas.org/sgp/isoo/isoodir1a.html

3. Computer Redaction
"…[i]f technically feasible, the amount of the information deleted shall be indicated at the place in the record where such deletion is made." Id. However, its terms are not limited to information maintained in electronic form, so it also codifies the sound administrative practice of marking records to show all deletions when records are disclosed in conventional paper form. "

Source: U.S. Department of Justice. "Congress Enacts E-FOIA Amendments."
http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page1.htm

**Red/Black Concept**
Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information, in electrical signal form, from those which handle unclassified (BLACK) information in the same form.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995.
http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

**Reference Material**
Documentary material over which the GCA, who lets the classified contract, does not have classification jurisdiction, and did not have classification jurisdiction at the time the material was originated. Most material made available to contractors by the DTIC and other secondary distribution agencies is reference material as thus defined.

Source: DoD. *National Industrial Security Manual* (NISPOM). DoD 5220.22-M, February 28, 2006,
https://www.dss.mil/GW/ShowBinary/DSS/isp/fac_clear/download_nispom.html

**Regional Information Sharing System (RISS)/RISSNET**
An established system of six regional centers that are used to "share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines." The RISS Program was created to combat traditional law enforcement targets, such as

drug trafficking and violent crime, but has been expanded to include other activities, such as terrorism and cybercrime.

The RISS system has created riss.net, the only secure internet-based national network for sharing of criminal intelligence among federal, state, and local law enforcement agencies. RISS also operates secure WATS/patch and telephone communications for one-on-one contact with RISS. RISS databases can provide criminal intelligence information and referral contacts for information exchange with other member agencies.

Source: Harold C. Relyea and Jeffrey W. Seifert. "Information Sharing for Homeland Security: A Brief Overview." *CRS Report to Congress* January 10, 2005, http://www.fas.org/sgp/crs/RL32597.pdf ; Attorney General Ashcroft's "Memorandum to all U.S. Attorneys." November 13, 2001; "Review of United States Attorneys' Offices' Use of Intelligence Research Specialists. " December 2005, http://www.usdoj.gov/oig/reports/EOUSA/e0603/final.pdf and Department of Justice. Bureau of Justice Assistance. *Intelligence-Led Policing: The New Intelligence Architecture,* http://www.ncjrs.gov/pdffiles1/bja/210681.pdf

**Regrade**
A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such a different degree of protection.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

**Relevant Evidence**
Evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

Source: Article 101. Rule 401. Federal Rules of Evidence, http://www.law.cornell.edu/rules/fre/rules.htm

**Relevant Information**
All information of importance to commanders and staffs in the exercise of command and control.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Restricted**
Reports that at an earlier date were classified sensitive or confidential and the need for high-level security no longer exists; and

Nonconfidential information prepared for/by law enforcement agencies.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404

**Restricted Collateral Information**

This Directive also covers programs other than SCI or special access programs that impose controls governing access to classified intelligence information or control procedures beyond those normally provided for access to Confidential, Secret, or Top Secret information, and for which funding is specifically identified. This Directive does not cover access controls for human or organizational sources.

Source: Director of Central Intelligence. Controlled Access Program Oversight Committee June 2, 1995., http://www.fas.org/irp/offdocs/D.C.id3-29.html

**Restricted Data (RD)**

***See Born Classified***

1. All data concerning the following, but not including data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act:

design, manufacture, or utilization of atomic weapons;
production of special nuclear material; or
use of special nuclear material in the production of energy
mass or dimensions of fissile materials, pits, or nuclear assembly systems
efficiency of nuclear materials
boosting systems
initiator design
test information revealing RD
naval nuclear propulsion information
radiological warfare

RD is Born Classified.

Source: The McMahon Act (AEC, 1954)
http://www.hr.lanl.gov/SCourses/All/PortionMarking/define.htm; Arvin S. Quist. Chapter 3. "Classification of Information," http://www.fas.org/sgp/library/quist2/chap_3.html; Quist, "Principles for Classification of Information," http://www.fas.org/sgp/library/quist2/index.html; DOE, *Understanding Classification*. Washington, D.C.: Assistant Secretary for Defense Programs, Office of Classification, 1987, SUDOC:E 1.15:0007/1; and Energy. 10 CFR 1045, http://www.gpoaccess.gov/CFR/index.html

2. Only DOE, NRC, DoD, and NASA can grant access to RD and FRD. Contractors of all other federal agencies must be processed for PCLs (personnel clearance) by the DOE. The minimum investigative requirements and standards for access to RD and FRD are set forth in the *National Industrial Security Program Operating Manual* (NISPOM), Chapter 9.

Source: DoD. *National Industrial Security Program Operating Manual* (NISPOM). DoD 5220.22-M. Chapter 9. January 1995, http://www.fas.org/sgp/library/nispom/chap_09.htm

3. E.O. 12958, amended, does not apply to RD or FRD.

Source: Information Security Oversight Office. Marking Classified National Security Information Booklet. ISOO Implementing Directive No. 1 Effective September 22, 2003, http://www.archives.gov/isoo/training/marking-booklet.pdf

**Reveal**

*See Data Mining*

Internal Revenue Service. Will be used to detect financial criminal activity such as tax evasion;
Purpose: Detecting criminal activities or patterns;
Status: Planned;
Features: Personal information: Yes;
Features: Private sector data: Yes;
Features: Other agency data: No.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004. http://www.gao.gov/htext/d04548.html

**Reverse FOIA**

A "reverse" FOIA action is one in which the "submitter of information, usually a corporation or other business entity"' that has supplied an agency with "data on its policies, operations or products, seeks to prevent the agency that collected the information from revealing it to a third party [usually] in response to the latter's FOIA request."

Source: U.S. Department of Justice. *Freedom of Information Act Guide*, http://www.usdoj.gov/oip/reverse.htm

**Revolution in Military Affairs (RMA)**

Dramatic changes in the art of warfare precipitated by rapid technological advances. Exploiting the RMA means not only acquiring new systems based on advanced technology but also developing the concepts, doctrine, and organizations to fully utilize the new technologies in a way to dominate the battlefield.

Source: Defense Acquisition University. *Glossary: Defense Acquisition Acronyms and Terms.* 11th ed., 2003, http://www.dau.mil/pubs/Glossary/preface.asp

**Reynard**

A seedling effort to study the emerging phenomenon of social (particularly terrorist) dynamics in virtual worlds and large-scale online games and their implications for the Intelligence Community. The cultural and behavioral norms of virtual worlds and gaming are generally unstudied. Therefore, Reynard will seek to identify the emerging social, behavioral and cultural norms in virtual worlds and gaming environments. The project would then apply the lessons learned to determine the feasibility of automatically detecting suspicious behavior and actions in the virtual world.

Source: DNI, *Data Mining Report*, February 15, 2008, http://www.fas.org/irp/dni/datamining.pdf

**Right-to-Know**

1. "It seems to me that 'the Right to Know' should be the phrase, because it represents the people's right, as it actually is, and not merely a selfish right of printers alone, as it is not. It means that the government may not, and the newspapers and broadcasters should not, by any method whatever curb delivery of any information essential to the public welfare and enlightenment. To do so should constitute malfeasance and be punishable. If the First Amendment to the American constitution were being written now it well could be worded: 'Congress shall make no law…abridging the Right to Know through oral or printed word or any other mans of communicating ideas or intelligence.' What is needed today is a constitutional amendment that would more properly state what is really meant in connection with this freedom by which newspapers and radio function for the people."

Source: Kent Cooper. *The Right to Know: An Exposition of the Evils of News Suppression and Propaganda.* New York: Farrar, Straus and Cudahy, 1956. 1617, and "Right to Know" editorial. *New York Times* January 23, 1945, p.18.

2. The people's right to know is really a composite of several rights. It has at least five broad, discernible components: 1. the right to get information; 2. the right to print without prior restraint; 3. the right to print without fear of reprisal not under due process; 4. the right of access to facilities and material essential to communication; and 5. the right to distribute information without interference by government acting under law or by citizens acting in defiance of the law.

Source: James Russell Wiggins. *Freedom or Secrecy*? New York: Oxford University Press, 1956. 3-4.

3. Reduced to its simplest terms the concept includes two closely related features: First, the right to read, to listen, to see, and to otherwise receive communications; and second, the right to obtain information as a basis for transmitting ideas or facts to others. Together these constitute the reverse side of the coin from the right to communicate. But the coin is one piece, namely the system of freedom of expression.

Source: Emerson, Thomas I. "Legal Foundations of the Right to Know Symposium: The First Amendment and the Right to Know." 1976 Wash. U. L. Q. (1976) 1-25.

4. Requestor has official capacity and statutory authority to the information being sought.

Source: David L. Carter. Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies. Dept. of Justice, Office of Community Oriented Policing Services, 2004., http://www.cops.usdoj.gov/default.asp?Item=1404

**Included here are regulatory mandates for public disclosure of various types of information. This is not an exhaustive list**:

Community Right to Know (RTK) | Toxic Release Inventory

1. In response to the Bhopal accident, the United States reauthorized and expanded the Superfund Amendments and Reauthorization Act of 1986 (SARA) to include the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA), which increased the public's right to know about chemical hazards, chemical emergencies, and chemical releases in their communities. [54]

The purpose of RTK is to "increase community awareness of chemical hazards and to facilitate emergency planning" through Emergency Planning (Sections 301-303), Emergency Release Notification (Section 304), Community Right-to-Know Reporting Requirements (Sections 311-312), and Toxic Release Inventory Reporting (Section 313). However, only certain companies within a SIC (Standard Industrial Classification Code) are obliged to report; the current TRI toxic chemical list currently includes over 650 individually listed chemicals and chemical categories out of the approximately 70,000-100,000 chemicals used in commerce, and the approximately one thousand additional chemicals introduced annually.[55]

Source: EPA, http://www.epa.gov/epahome/r2k.htm

2. The EPA is considering changes to the TRI: changes in reporting requirements from the current annual reporting requirement to every other year reporting all facilities, and allows

[54] More than 3,400 Indians died (conservative estimates - another estimate is 8,000 http://www.bhopal.net/oldsite/poisonpapers.html ) and more than 200,000 individuals injured when methyl isocyanate was released from Union Carbide's Bhopal insecticide plant in 1984. See http://www.bhopal.org/

[55] In its reporting on "reducing burden associated with facility reporting" to the Toxics Release Inventory, EPA (31) writes: "the objective is to *reduce the amount of information*, [emphasis added] and therefore the amount of time, required of facilities to comply with TRI, and if warranted, to relieve certain facilities (e.g., certain small businesses) of reporting requirements altogether." OIRA's Fiscal Year 2005 *Managing Information Collection*: *Information Collection Budget of the United States*: http://www.whitehouse.gov/OMB/inforeg/2005_icb_final.pdf.

facilities to withhold information on low-level production of persistent bioaccumulative toxins (PBTs), including lead and mercury.

There is a fascinating discussion of "Burden Methodology" on page 57827.

Source: EPA. "TRI Burden Reduction Proposed Rule." *Federal Register* October 4, 2005, http://edocket.access.gpo.gov/2005/pdf/05-19710.pdf.

- Ethics in Government Act of 1978

Requires the filing of detailed financial statements by federal government officials to be filed with an Office of Government Ethics, which reviews them to see if there is a conflict between an individual's public job and his private holdings. The statements are considered public documents.

Advisory committees covered by the Act must open their meetings under the Government in the Sunshine Law as well as disclose their records as required by the Freedom of Information Act.

Source: Steven Goldberg, "Public Access to Government Information": http://usinfo.org/enus/media/pressfreedom/freedom6.htm and 5 U.S.C. App. http://www.access.gpo.gov/U.S.C.ode/title5a/5a_3_.html

- Federal Advisory Committee Act (FACA)

1. Mandates that each advisory committee meeting shall be open to the public, advisory committee proceedings published in the *Federal Register*, and disclose their records as required by the Freedom of Information Act.

Source: Public Law 92-463, Oct. 6, 1972. 5 U.S.C., Appendix. http://www.access.gpo.gov/U.S.C.ode/title5a/5a_1_.html and Stephanie Smith, "Federal Advisory Committees: A Primer," Updated March 20, 2007, *CRS Report for Congress* RL30260, http://www.fas.org/sgp/crs/misc/RL30260.pdf

2. S.1873 "To prepare and strengthen the biodefenses of the United States against the deliberate, accidental, and natural outbreaks of illness, and for other purposes" restricts FACA (Federal Advisory Committee Act) access to information and meetings (111).

Source: S.1873 "To prepare and strengthen the biodefenses of the United States against the deliberate, accidental, and natural outbreaks of illness, and for other purposes." October 17, 2005. Text at GPO Access http://frwebgate.access.gpo.gov (**10/17/2005: 12/11/05** Read twice and referred to the Committee on Health, Education, Labor, and Pensions. (text of measure as introduced: CR S11424-11433)

- Government in the Sunshine Act

Regulatory guidance for public meetings; agencies "shall make promptly available to the public, in a place easily accessible to the public, the transcript, electronic recording, or minutes (as required by paragraph (1)) of the discussion
of any item on the agenda, or of any item of the testimony of any witness received at the meeting, except for such item or items of such discussion or testimony as the agency determines to contain information which may be withheld under subsection (c). Copies of such transcript, or minutes, or a transcription of such recording disclosing the identity of each speaker, shall be furnished to any person at the actual cost of
duplication or transcription. The agency shall maintain a complete verbatim copy of the transcript, a complete copy of the minutes, or a complete electronic recording of each meeting, or portion of a meeting, closed to the public, for a period of at least two years after such meeting, or until one year after the conclusion of any agency proceeding
with respect to which the meeting or portion was held, whichever occurs later.

Source: Government Organization and Employees. "Open Meetings." 5 U.S.C. 552b. http://www.gpoaccess.gov/uscode/browse.html and Steven Goldberg "Public Access to Government Information." http://usinfo.org/enus/media/pressfreedom/freedom6.htm

- Security and Exchange Commission (SEC)

SEC established requirements for continuous disclosure in forms 10-K, 10-Q, 8-K, etc.

Source: "Commodity and Securities Exchanges." Regulation S-K, 17 CFR 229, http://www.gpoaccess.gov/CFR/index.html

**Risk Assessment and Horizon Scanning (RAHS)**

***See Total Information Awareness (TIA)***

While different in design from TIA, the RAHS system shares some intellectual roots with the doomed Darpa effort....RAHS as a system that monitors multiple feeds of data -- both open and classified -- to detect possible threats. "Essentially it's a strategic tool that ties together every one of the agencies in a government into a large network that is constantly scanning the horizon looking for weak signals that point toward the possibility of a significant event that would have important implications for Singapore," he [*sic* Peterson] said.

Source: Sharon Weinberger, "Son of TIA: Pentagon Surveillance System Is Reborn in Asia," *Wired* March 22, 2007, http:/www.wired.com/politics/onlinerights/news/2007/03/SINGAPORE?currentPage=1

**Routine Use**

1. A *routine use* is a term from the Privacy Act of 1974. It means "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."

Source: 5 U.S.C. 552a (a) (7). The Privacy Act of 1974 http://www.usdoj.gov/opcl/privstat.htm and EPIC, http://www.epic.org/privacy/1974act/

2. One of the primary objectives of the Act is to restrict the use of information to the purposes for which it was collected. The term "routine use" was introduced to recognize the practical limitations of restricting use of information to explicit and expressed purposes for which it was collected. It recognizes that there are corollary purposes "compatible with the purpose for which [the information] was collected" that are appropriate and necessary for the efficient conduct of government and in the best interest of both the individual and the public.

Source: "Office of Management and Budget Privacy Act Implementation Guidelines and Responsibilities" (July 9, 1975), http://www.defenselink.mil/privacy/1975OMB_PAGuide/75JULY09.pdf

3. An agency can adopt a routine use after publishing the routine use for public comment in the Federal Register.

Source: 5 U.S.C. 552a (e) (11). The Privacy Act of 1974, http://www.usdoj.gov/opcl/privstat.htm and EPIC, http://www.epic.org/privacy/1974act/ [definitions contributed by Robert Gellman, http://www.bobgellman.com/].

**Ruse**

***See Deception***

In military deception, a trick of war designed to deceive the adversary, usually involving the deliberate exposure of false information to the adversary's intelligence collection system.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

---

## ~ S ~

**Safeguards Information (SGI)**

1. Information not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed, (1) security measures for the physical protection of special nuclear material, or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities.

Source: Energy. 10 CFR 73, http://www.gpoaccess.gov/CFR/index.html

2. A special category of sensitive unclassified information to be protected from unauthorized disclosure under section 147 of the Atomic Energy Act of 1954, as amended (AEA). Although SGI is considered to be sensitive unclassified information, it is handled and protected more like classified National Security Information than like other sensitive unclassified information (e.g., privacy and proprietary information).

Source: Atomic Energy Act of 1954 http://www.nrc.gov/;
Nuclear Regulatory Commission. "Physical Protection of Plants and Materials." 10 CFR 73, http://www.gpoaccess.gov/fr/index.html and *Federal Register* October 31, 2006, http://www.gpoaccess.gov/fr/index.html

3. Safeguards Information--Modified Handling (SGI-M). SGI-M pertains to certain SGI subject to handling requirements that are modified from what part 73 itself currently requires. This designation for SGI applies to certain quantities of source, byproduct, and special nuclear materials for which the risk of unauthorized disclosure of information is relatively low.

Source: *Federal Register February* 11, 2005 (Volume 70, Number 28), Page 7196-7217, http://www.gpoaccess.gov/fr/index.html

**Safeguarding**
Measures and controls that are prescribed to protect classified information.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information."
http://www.archives.gov/federal-register/executive-orders/2003.html

**Sanitization**
***See Redaction***
The process of editing, or otherwise altering, intelligence or intelligence information to protect sensitive sources, methods, and analytical capabilities so as to permit greater dissemination of the data.

Source: DoD. Instruction 5210.52. "Security Classification of Airborne Sensor Imagery and Imaging Systems." May 18, 1989, http://www.dtic.mil/whs/directives/corres/pdf/521052p.pdf

**Sanitize**
Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**SCAME**

Acronym used to remember the steps in analyzing opponent propaganda. The letters stand for "source, content, audience, media, effects."

Source: DoD. *Psychological Operations,* FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

**Secondary Censorship**

Armed forces censorship performed on the personal communications of officers, civilian employees, and accompanying civilians of the Armed Forces of the United States, and on those personal communications of enlisted personnel of the Armed Forces not subject to Armed Forces primary censorship or those requiring reexamination.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Secret Protocol Router Network (SIPRNET)**

Provides secure classified Secret communications; access to Secret counterterrorism reports, data, and analysis; and the capability to communicate electronic national security data among the USAO [United State Attorney Offices] districts, other components, and other law enforcement and national security agencies.

Source: Review of United States Attorneys' Offices' Use of Intelligence Research Specialists. December 2005, http://www.usdoj.gov/oig/reports/EOUSA/e0603/final.pdf

**Secrecy**

1. Secrecy simply means that a document is not available when you need it.

Source: James Werner. "Secrecy and its Effect on Environmental Problems in the Military: An Engineer's Perspective." *New York University Environmental Law Journal* 2 no. 2 (1993): 351-359, http://www1.law.nyu.edu/journals/envtllaw/issues/vol2/index.html

2. Secrecy is a form of government regulation. There are many such forms, but a general division can be made between regulations dealing with domestic affairs, and those dealing with foreign affairs. In the first category, it is generally the case that government prescribes what the citizen may do; in the second category, it is generally the case that government prescribes what the citizen may know.

Source: Report of the Commission on Protecting and Reducing Government Secrecy ("Moynihan Commission"), Senate Document 105-2, 1997. "Secrecy: a Brief Account of the American Experience." http://www.fas.org/sgp/library/moynihan/appa1.html

3. The compulsory withholding of knowledge, reinforced by the prospects of sanctions for disclosure.

Source: Edward A. Shils. *The Torment of Secrecy: The Background and Consequences of American Security Policies*. Glencoe, IL: The Free Press, 1956.

4. Anything that "is kept intentionally hidden, set apart in the mind of its keeper as requiring concealment."

…"Conflicts over secrecy…are conflicts over power: the power that comes through controlling the flow of information."

Source: Sissela Bok. *Secrets*. New York: Vintage Books, 1989. 5,19.

5. Consciously willed concealment.

Source: Simmel, Georg. "The sociology of secrecy and secret societies." *American Journal of Sociology* 11 no.4 (1906): 441-498.

6. "…a tampering of communications." Political and governmental secrecy consists of the process of secreting information about political entities, especially when that information has significant implications for rival entities of the general public."

Source: Friedrich, Carl. "Nature and function of secrecy and propaganda." Ed. Susan L. Maret and Jan Goldman. Government Secrecy: Classic and Contemporary readings. Westport, CT: Libraries Unlimited, 2008. 85-86.

**Types of Secrecy**

**Note that many of these types of secrecy have no established definition:**

**Bureaucratic Secrecy,** which refers to the largely unconscious hoarding and withholding of information that characterizes all bureaucracies, as classically described by Max Weber. Unlike political secrecy, there is no particular advantage to be gained from bureaucratic secrecy, nor is there a persuasive national security rationale.

Source: Steven Aftergood. "Secrecy is Back in Fashion." *Bulletin of the Atomic Scientists* November-December 2000. http://www.thebulletin.org/article.php?art_ofn=nd00aftergood

**Essential Secrecy**

The condition achieved from the denial of critical information to adversaries.

Source: Department of Defense. *DoD of Military and Associated Terms* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Genuine National Security Secrecy** pertains to that body of information which, if disclosed, could actually damage national security in some identifiable way. Of course, this description begs the crucial questions of what "national security" is, what constitutes "damage," and how the meaning of these two terms may change over time. But without attempting to conclusively define national security, common sense suggests that this category includes things like design details of advanced military technologies, as well as those types of information that must remain secret in order for authorized diplomatic and intelligence functions to be performed. The sensitivity of this kind of information is the reason we have a secrecy system in the first place, and when it is working properly the system positively serves the public interest.

Source: Steven Aftergood. "Secrecy is Back in Fashion." *Bulletin of the Atomic Scientists* November-December 2000. http://www.thebulletin.org/article.php?art_ofn=nd00aftergood

**Government Secrecy**

With the exception of the procedures for classifying "nuclear-related information" under the Atomic Energy Act and protecting intelligence "sources and methods" under the National Security Act, the mechanics for protecting national security information have evolved through a series of executive orders. Over the past half century, the Congress has played only a limited role in any consideration of how the system should function, limiting itself to occasional oversight hearings. The Executive Branch has assumed the authority both for structuring the classification system and for deciding the grounds upon which secrets should be created and maintained. Thus, what commonly is referred to as 'government secrecy' more properly could be termed 'administrative secrecy' or 'secrecy by regulation.'

Source: Report of the Commission on Protecting and Reducing Government Secrecy ("Moynihan Commission"), Senate Document 105-2, 1997, http://www.fas.org/sgp/library/moynihan/chap1.html

**Intelligence Secrecy**

The October 30 ODNI news release went on to insist that "Any and all subsidiary information concerning the National Intelligence (NIP) budget will not be disclosed as such disclosures could harm national security."

"Any and all subsidiary information"? This implies, for example, that if a breakdown of the amount of money spent by the intelligence community on declassification activities were published, it "could harm national security." But that hardly seems likely.

In a candid moment last year, ODNI officials admitted that they really don't know why they classify all the things that they do. "There is wide variance in application of classification levels," an internal January 2008 ODNI study (pdf) obtained by Secrecy News found. "The definitions of 'national security' and what constitutes 'intelligence' -- and thus what must be classified -- are unclear."

Source: *Secrecy News*, FAS Project on Government Secrecy Issue No. 87, November 2, 2009 http://www.fas.org/blog/secrecy/

**Invention Secrecy**

Whenever publication or disclosure by the grant of a patent on an invention in which the Government has a property interest might, in the opinion of the head of the interested Government agency, be detrimental to the national security, the Commissioner upon being so notified shall order that the invention be kept secret and shall withhold the grant of a patent therefor under the conditions set forth hereinafter.

Whenever the publication or disclosure of an invention by the granting of a patent, in which the Government does not have a property interest, might, in the opinion of the Commissioner, be detrimental to the national security, he shall make the application for patent in which such invention is disclosed available for inspection to the Atomic Energy Commission, the Secretary of Defense, and the chief officer of any other department or agency of the Government designated by the President as a defense agency of the United States. Each individual to whom the application is disclosed shall sign a dated acknowledgment thereof, which acknowledgment shall be entered in the file of the application.

Source: Invention Secrecy Act of 1951, http://www.fas.org/sgp/othergov/invention/35usc17.html, FAS, "Invention Secrecy," http://www.fas.org/sgp/othergov/invention/index.html, *Secrecy News* FAS Project on Government Secrecy. Issue No. 83, October 22, 2009, http://www.fas.org/blog/secrecy/

**Nuclear Secrecy**

***See Information Crime, Information Criminal, Leaks***

The intentional blocking, compartmentalizing, concealment, control, distorting, hoarding, censoring, and manipulation of information related to the numerous dimensions of historic and ongoing atomic or nuclear fuel cycle activities, including access to information related to pollution, risk, public health, waste, and weapons development. *Nuclear secrecy* is institutionalized through bureaucratic organization, statute, regulation, decree, security classification of information, language, control of the media, and informal practices, carrying with it some type of penalty for disclosure such as harassment, monetary fines, incarceration, and other means of silencing individuals.

I base my definition on Sissela Bok's (1989) work on secrecy as the intentional concealment and blocking of information, sociologist Edward Shils' (1956) idea of secrecy as the "compulsory withholding of knowledge, reinforced by the prospects of sanctions for disclosure, " Steven Aftergood's characterization of specific types of secrecy [this section], and recent developments involving reclassification of Cold War weapons data. This definition is also based on the penalties for disclosure of "atomic" information under the U.S. Atomic Energy Act of 1948 and 1954, as well as the laws of other countries [the UK and Russian Federation, for example].

Source: Definition, Maret[56]; Bok, *Secrets: On the Ethics of Concealment and Revelation*. [New York: Vintage Books]; Shils, *The Torment of Secrecy* [Glencoe, IL: The Free Press]; William Burr, Thomas S. Blanton, and Stephen I. Schwartz. "The Costs and Consequences of Nuclear Secrecy," [In Stephen Schwartz, (ed.) *Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons Since 1940*. Brookings Institute, 1998. 433-483]; National Security Archive Briefing Book, William Burr (ed*.). How Many and Where Are the Nukes*, August 18, 2006, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB197/index.htm, Steven Aftergood and Frank N. von Hippel, "The U.S. Highly Enriched Uranium Declaration: Transparency Deferred but not Denied," http://cns.miis.edu/pubs/npr/vol14/141/141aftergood.pdf, Carroll Quiqley, "Nuclear rivalry and the Cold War: 1945-1950," *Tragedy and Hope: A History of the World in Our Time* [Macmillan, 1966], and Gar Alperovitz, *The Decision to Use the Atomic Bomb and the Architecture of an American Myth* [esp. chapter 48, 'Censorship and Secrecy," Knopf, 1995].

**Political Secrecy**, which refers to the deliberate and conscious use of classification authority for political advantage, irrespective of any threat to national security. Typically, the intent here is to shield an official or a vulnerable program from embarrassment or controversy.

This is the smallest of the three categories but it is the most dangerous to the political health of the nation. For example, some of the early research on the effects of radiation exposure on human subjects was explicitly classified to evade public controversy and legal liability. [2] More recently, the classification of a letter written by MIT Professor Ted Postol critical of missile defense technology was most likely an instance of political secrecy. [3]

Source: Steven Aftergood. "Secrecy is Back in Fashion." *Bulletin of the Atomic Scientists* November-December 2000, http://www.thebulletin.org/article.php?art_ofn=nd00aftergood

**Retroactive Secrecy**
***See Reclassification***

1. In *United States of America, Plaintiff v. The Progressive Inc.*, Erwin Knoll, Samuel Day, Jr., and Howard Morland, Defendants, the Plaintiff "advanced the concept of retroactive secrecy, declaring that previously published articles contained secrets."

Source: Stephen Hilgartner, Richard C. Bell, and Rory O'Connor. *Nukespeak*. New York: Penguin Books, 1982. 66-71.

2. The government argues that its national security interest also permits it to impress classification and censorship upon information originating in the public domain, if when drawn together, synthesized and collated, such information acquires the character of presenting immediate, direct and irreparable harm to the interests of the United States.

Defendants contend that the projected article merely contains data already in the public domain

[56] Thanks to Ronald A. Hardert Ph.D. for his assistance in helping me flesh out the specifics of nuke secrecy.

and readily available to any diligent seeker. They say other nations already have the same information or the opportunity to obtain it. How then, they argue, can they be in violation of 42 U.S.C. §§ 2274(b) and 2280 which purport to authorize injunctive relief against one who would disclose restricted data "with reason to believe such data will be utilized to injure the United States or to secure an advantage to any foreign nation . . ."?

Although the government states that some of the information is in the public domain, it contends that much of the data is not, and that the Morland article contains a core of information that has never before been published. Furthermore, the government's position is that whether or not specific information is "in the public domain" or has been "declassified" at some point is not determinative. The government states that a court must look at the nature and context of prior disclosures and analyze what the practical impact of the prior disclosures are as contrasted to that of the present revelation.

The government feels that the mere fact that the author, Howard Morland, could prepare an article explaining the technical processes of thermonuclear weapons does not mean that those processes are available to everyone. They lay heavy emphasis on the argument that the danger lies in the exposition of certain concepts never heretofore disclosed in conjunction with one another.

Source: *United States of America, Plaintiff, v. The Progressive Inc.*, Erwin Knoll, Samuel Day, Jr., and Howard Morland, Defendants, 467 *F. Supp*. 990 and 486 *F. Supp*. 5*;* Michael Macdonald Mooney, ""Right Conduct" for a 'Free Press': the Containment of Secrets," *Harper's Magazine* 260 (March 1980): 35-45, and *The Progressive* November 1979 issue "The H-Bomb Secret: How We Got It and Why We're Telling it," issue online at: http://progressive.org/?q=node/2252

**Secrecy in the Public Interest,** Not defined. This statute amends the Housekeeping Statute, establishes agency communication of rules and activities via the *Federal Register.* "Public Information." Sec. 3. Except to the extent that there is involved (1) any function of the United States requiring secrecy in the public interest or (2) any matter relating solely to the internal management of an agency

Source: 60 U.S. Statutes at Large 238 (1946) and Louis Fisher. *In the Name of National Security: Unchecked Presidential Power and the Reynolds Case*. Lawrence: University Press of Kansas, 2006.

**Structural Secrecy**

The way that patterns of information, organizational structure, processes, and transactions, and the structure of regulatory relations systematically undermine the attempts to know and interpret situations in all organizations. At NASA, structural secrecy concealed the seriousness of the O-ring problem, contributing to the persistence of the scientific paradigm on which the belief in acceptable risk was based.

Source: Vaughan, Diane. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA.* Chicago: University of Chicago Press, 1996.

### Tacit Silence, or a Partial Secret

Thompson (3) has written on a type of secrecy he calls *tacit silence*, or *a partial secret*. This type of secrecy is somewhere between deep concealment and full disclosure, and based on the philosophy things are better left unsaid. Thompson writes "such secrets are not completely concealed because their content may be widely known or could be widely known. But their content is not made explicit, and its not being made explicit is necessary" for a policy's effectiveness. Thompson has identified three kinds of tacit silences/partial secrets:

Excuses and Nonenforcement | Compelled Silence | Political Hypocrisy

Source: Dennis F. Thompson. "Democratic Secrecy." *Political Science Quarterly* 114 no. 2 (1999): 181-193.

### Trade Secrets

1. Any confidential formula, pattern, process, device, information or compilation of information that is used in an employer's business, and that gives the employer an opportunity to obtain an advantage over competitors who do not know or use it.

Source: "Crimes and Criminal Procedure." 29 CFR 1910.1200; Appendix D (CFR) sets out the criteria to be used in evaluating trade secrets. http://www.gpoaccess.gov/CFR/index.html

2. "The Economic Espionage Act of 1996" made the theft of trade secrets a federal criminal offense. Economic espionage, as described in §1831, refers to foreign power-sponsored or -coordinated intelligence activity, directed at the U.S. government or corporations, entities, or other individuals operating in the United States, for the purpose of unlawfully obtaining trade secrets Under the Act, the FBI's National Counterintelligence Center has authority to prosecute trade secret theft in the United States, international and on the Internet.

Source: 18 U.S.C. §§ 1831-1839, and Patrick W. Kelley. "The Economic Espionage Act of 1996." http://www.fbi.gov/publications/leb/1997/july976.htm

- **Various former KGB IC definitions of secrecy**

*Sekretnaya informatsiya*

information and data whose open publication and discussion is forbidden by authorities and constitutes sate secrets, and information contained in official documents and in scientific training materials which bear a secrecy classification.

*Sekretnost*

a substantial characteristics of a piece of information, which determines the degree of protection which the adversary gives it to prevent disclosure.

*Taynopis; secret writing*
The various means of producing invisible manuscripts and typed texts which can only be read after special processing.

Source: Vasily Mitrokhin, ed. *KGB Lexicon: The Soviet Intelligence's Officer's Handbook*. London: Frank Cass, 2002.

## Secrecy Oaths

House and Senate requirements differ with regard to secrecy oaths. At the beginning of the 104th Congress, the House adopted a secrecy oath for all Members, officers, and employees of the chamber. Before any such person may have access to classified information, he or she must "solemnly swear (or affirm) that I will not disclose any classified information received in the course of my service with the House of Representatives, except as authorized by the House of Representatives or in accordance with its Rules" (House Rule XXIII, clause 13, 108th Congress). Previously, a similar oath was required only for members and staff of the House Permanent Select Committee on Intelligence; this requirement had been added in the 102nd Congress as part of the Select Committee's internal rules, following abortive attempts to establish it in public law.

Source: Frederick M. Kaiser. "*Protection of Classified Information by Congress: Practices and Proposals*." *CRS Report to Congress* January 11, 2006, http://www.fas.org/sgp/crs/RS21900.pdf

## Secrecy Order

***See Invention Secrecy, Patents***

The U.S. Patent & Trademark Office (PTO) is responsible for reviewing patent applications and imposing secrecy orders when disclosure of an invention by publication of a patent would be detrimental to the national security. A secrecy order withholds the grant of a patent, orders that the invention be kept in secrecy and restricts filing of foreign patent applications.

A type 1 secrecy order applies to patent applications containing unclassified subject matter that cannot be lawfully exported under existing U.S. export control laws without government approval. A type 1 secrecy order is only imposed upon recommendation from the Department of Defense.

The intent of a type 2 secrecy order is to treat classified/classifiable information in a patent application in the same manner as any other classified material under the ISM. Accordingly, this secrecy order includes notification of the classification level of the technical data in the application, and provides a level of protection at that classification level.

A type 3 secrecy order is used for patent applications which contain technical data that would be classified based upon its technical content, but cannot be classified or placed under a type 2 secrecy order because there is no known government property interest in the invention.

Source: FAS. "The Secrecy Order Program in the United States Patent & Trademark Office" (Rev. 6/27/91) http://www.fas.org/sgp/othergov/invention/program.html, and Herbert N. Foerstel. *Secret Science: Federal Control of American Science and Technology.* Westport, CT: Praeger, 1993. 168-172.

**Secret**

***See Classification***

1. The classification level between Confidential and Top Secret applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

Source: Los Alamos National Lab. "Definitions." http://www.hr.lanl.gov/SCourses/All/PortionMarking/define.htm

**Secret-Cleared U.S. Citizen**

A citizen of the United States who has undergone a background investigation by an authorized U.S. Government Agency and been issued a Secret security clearance in accordance with Executive Orders 12968 and 10450 and implementing guidelines and standards published in 32 CFR Part 147.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003. http://www.state.gov/m/a/dir/regs/

**Secret Restricted Data**

***See Born Classified, Restricted Data***

Information classified as Secret Restricted Data is simply whatever the DOE classification office rules as classified. It make no difference if the same information is well known in open scientific journals; if the DOE says that something is classified it remains SRD even though every citizen in the country can read it in a physics journal or physics textbook.

Source: Hugh E. Dewitt. "Statement." United States. Congress. House. Committee on Government Operations. Subcommittee on Government Information and Individual Rights. *The Government's Classification of Private Ideas.*, (Hearings before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-sixth Congress, second session, February 28, March 20, and August 21, 1980. 550. SUDOC: Y 4.G 74/7:G 74/5); also see "Joint Statement for the House Subcommittee on Government Information and Individual Rights," G.E. Marsh, A. de Volpi, T.A. Postol, and G.S. Stanford, 561-571.

**Secure Collaborative Operational Prototype Environment/Investigative Data Warehouse**

***See Data Mining***

Federal Bureau of Investigation. Allows the FBI to search multiple data sources through one interface to uncover terrorist and criminal activities and relationships. Data sources are a combination of structured and unstructured text;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004. http://www.gao.gov/htext/d04548.html

**Secure Flight (Test Records)** [57]

***See Passenger Name Record Data***

1. Secure Flight involves the submission of a limited amount of passenger information by an aircraft operator to TSA whenever a reservation is made for a flight in which the origin and destination are domestic airports. It is important to note that the information collected by the aircraft operators and submitted to TSA will be used solely for the purpose of comparing a subset of the passenger reservation data to watch lists. No other use of the information is authorized. Under this new program, TSA will compare the identifying information of airline passengers contained in passenger name records (PNRs) to the identifying information of individuals in the Terrorist Screening Database of the Terrorist Screening Center (TSC).

Source: Transportation Safety Administration (TSA).[See the Wayback Machine @ http://www.archive.org/web/web.php http://www.tsa.gov/public/interapp/editorial/editorial_1716.xml; *Federal Register* 69 no.185 (September 24, 2004), http://www.gpoaccess.gov/fr/

2. Secure Flight was suspended in 2006. For background information, see the Electronic Privacy Information Center's Secure Flight page, http://epic.org/privacy/airtravel/secureflight.html

**Security Category**

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have an organizational operations, organizational assets, or individuals.

---

[57] The precursor to Secure Flight was the Computer Assisted Passenger Prescreening System (CAPPS II). See Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview" Updated January 18, 2007, http://opencrs.com/document/RL31798/2007-01-18

Source: FIPS (Federal Information Processing Standard) Publication 199. "Standards for Security Categorization of Federal Information and Information Systems." February 2004. http://www.csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

**Security Classification**
*See Classification*

**Security Classification Designations**
Refers to "Top Secret," and "Secret," and "Confidential" designations on classified information or material.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/

**Security Clearance(s)**
*See Nondisclosure Agreements*
1. **L Access Authorizations or Clearances**

a. L clearances permit an individual access, on a need-to-know basis, to Confidential Restricted Data, Secret and Confidential Formerly Restricted Data, Secret and Confidential National Security Information provided such information is not designated classified cryptographic information (CRYPTO), other classified communications security (COMSEC) information, or Sensitive Compartmented Information; and special nuclear material in quantities described in the DOE 5632 Order series, as required in the performance of official duties.

When L access authorizations or clearances are granted to employees of access permit holders, they are identified as L(X) access authorizations or clearances and permit access only to the type of Confidential Restricted Data specified in the access permit. Background checks not as stringent as in Q clearance.

Source: DOE. Personnel Security Program, http://www.fas.org/irp/DoDdir/doe/o5631_2c/o5631_2ca2.htm

b. L access authorization means an access authorization granted by the Commission that is normally based on a national agency check with a law and credit investigation (NACLC) or an access national agency check and inquiries investigation (ANACI) conducted by the Office of Personnel Management.

Source: Nuclear Regulatory Commission (NRC) 10 CFR § 25.5 "Definitions," http://www.gpoaccess.gov/CFR/index.html

c. The 1954 amended Atomic Energy Act gave rise to L clearance, and gray areas of information which are "intended to give industry readier access to data necessary to getting into the field."

Source: Herbert S. Marks and George F. Trowbridge. "The Control of Information under the Atomic Energy Act of 1954."*Bulletin of the Atomic Scientists* 11 no.4 (1955): 128-130.

2. **Q Access Authorizations or Clearances**

a. Q clearances permit an individual to have access, on a need-to-know basis, to Top Secret, Secret, and Confidential levels of Restricted Data, Formerly RD.

Q (Q Sensitive) Clearance allows access to: Top Secret Restricted Data ~Top Secret Formerly Restricted Data ~Top Secret National Security Information ~ Secret Restricted Data ~ Special Nuclear Material (Category I & II) ~ Exclusion Area Access

Q (Nonsensitive) Clearance gives access to less sensitive types of Special Nuclear Material. Individuals working with Q non-sensitive clearances also have armed guards stationed nearby.

Source: Los Alamos National Lab, http://www.lanl.gov/security/clearances/index.shtml

b. Q access authorization means an access authorization granted by the Commission normally based on a single scope background investigation conducted by the Office of Personnel Management, the Federal Bureau of Investigation, or other U.S. Government agency which conducts personnel security investigations.

Source: Nuclear Regulatory Commission (NRC) 10 CFR § 25.5 "Definitions," http://www.gpoaccess.gov/CFR/index.html

3. **Facility Security Clearance (FCL)**

Any firm or business under contract to the Department which require access to classified information will need a facility security clearance commensurate with the level of access required.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM570, "Industrial Security Program." http://www.state.gov/m/a/dir/regs/

4. **Secret Security Clearance**

Granted to those persons that have"need-to-know" national security information, classified at the Confidential or Secret level. It is generally the most appropriate security clearance for state and local law enforcement officials that do not routinely work on an FBI Task Force or in an FBI facility. A Secret security clearance takes the least amount of time to process and allows for escorted access to FBI facilities.

Source: Federal Bureau of Investigation (FBI). Security Clearance Process for State and Local Law Enforcement , http://www.fbi.gov/clearance/securityclearance.htm

5. **Top Secret Security Clearance**

A Top Secret clearance may be granted to those persons who have"need-to-know" national security information, classified up to the Top Secret level, and who need unescorted access to FBI facilities, when necessary. This type of clearance will most often be appropriate for law enforcement officers assigned to FBI Task Forces housed in FBI facilities. In addition to all the requirements at the Secret level, a background investigation, covering a 10-year time period, is required. Once favorably adjudicated for a Top Secret security clearance, the candidate will be required to sign a Non-Disclosure Agreement.

Source: Federal Bureau of Investigation (FBI). Security Clearance Process for State and Local Law Enforcement, http://www.fbi.gov/clearance/securityclearance.htm

6. Sometimes the CIA must grant regulators top secret clearances and brief inspectors fully on highly sensitive programs. The clearance check requires an extensive background investigation and, therefore, is a lengthier process than the routine compliance inspection described above. 9 The level and scope of access the Agency affords these regulators is equal to that granted to officials in the intelligence community who have a "need to know" certain classified security information to perform specialized national security functions. Protection of classified information has not conflicted with the EPA's performance of its compliance oversight in such instances.

Source: R. Bradford Stiles. "Environmental Law and the Central Intelligence Agency: Is There a Conflict Between Secrecy and Environmental Compliance?" *New York University Law Journal* 2 no. 2 (1993).[58] http://www1.law.nyu.edu/journals/envtllaw/issues/vol2/index.html

7. Security clearances and written nondisclosure agreements can be required for congressional staff but are handled differently by the Senate and House. The Senate Office of Security mandates such requirements for all Senate employees needing access to classified information. No comparable across-the-board requirement for security clearances or secrecy agreements exists for House employees. Security clearances for staff and nondisclosure agreements are required, however, for House offices that follow the provisions of Executive Order 12968, governing access in the executive branch.

[58] As Paul Wolfowitz's leaked memo of March 7, 2003 states environmental laws [CERCLA, Clean Air Act, Clean Water Act, Coastal Zone Management Act, ESA, Marine Protection, Research and Sanctuaries Act, Public Health Service Act, RCRA, Safe Water Drinking Act, & TSCA] authorize the President to exempt federal agencies from reporting requirements if it is determined the exemption is in the "paramount interest of the United States" and "necessary reasons of national security."

Source: Frederick M. Kaiser. "Protection of Classified Information by Congress: Practices and Proposals." *CRS Report to Congress* January 11, 2006. http://www.fas.org/sgp/crs/RS21900.pdf

8. The Nuclear Regulatory Commission (NRC) instituted new regulations to give individuals ("intervenors") associated with environmental and public interest organizations the ability to access classified information associated with NRC-regulated activities, such as "potential intervenors in a hearing for a potential high-level radioactive waste repository and (2) advanced reactor design vendors."

Intervenors will be issued a security clearance to facilities storing classified information, and a background check, as well as being informed "that unauthorized disclosure of classified information could result in civil or criminal penalties. A person seeking access to classified information must, in addition to having a security clearance, have a need to know the particular information being sought."

Source: "NRC Revises Regulations on Access to Classified Information." http://www.nrc.gov/reading-rm/doc-collections/news/2005/05-087.html

**Security Controls**

The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have an organizational operations, organizational assets, or individuals.

Source: FIPS (Federal Information Processing Standard) Publication 199. "Standards for Security Categorization of Federal Information and Information Systems." February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

**Security Index**

Custodial Detention cards will be known as Security Index. FBI agents were to continue "to investigate dangerous and potentially dangerous" citizens and aliens and to list them in the Security Index. Sensitive that his insubordination could be discovered, Hoover admonished FBI officials that this renamed list was to be "strictly confidential and should at no time be mentioned or alluded to in investigative reports or discussed with agencies or individuals outside the Bureau," with the exception of MID and ONI officials, "and then only on a strictly confidential basis."

July 13, 1943 Attorney General Biddle terminates the FBI's Custodial Detention list. Hoover formally complies with this order on August 14, 1943, but covertly directs FBI officials to change the name to Security Index.

Source: Athan Theoharis, ed. *The FBI: A Comprehensive Reference Guide*. Phoenix: Oryx Press, 1998. 21, 367.

**Security Label**

Information representing the sensitivity of a subject or object, such as its hierarchical classification (Confidential, Secret, Top Secret) together with any applicable nonhierarchical security categories (e.g., sensitive compartmented information, critical nuclear weapons design information).

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Securocracy | Securocrat**

***See National Security State***

1. Emphasis on (information) secrecy, security classification of information, the creation of new secrets, reclassification of information, and institutionalized practices of compartmented access and information exemption; Secrecy bureaucracy.

Source: Steven Aftergood, and Tom Blanton. "The Securocrats' Revenge." *The Nation* 269 no. 5 (1999): 20.

2. Weber's (1958: 233) observation that the concept of the official secret is the specific invention of the bureaucracy, and *nothing is so fanatically defended*.

Source: H. H. Gerth and C. Wright Mills, ed. and trans, *From Max Weber: Essays in Sociology*. New York: Oxford University Press, 1958.

**Segregable and Reasonably Segregable Information**

If a requested record contains material covered by an exemption and material that is not exempt, and it is determined under the procedures in this subpart to withhold the exempt material, any reasonably segregable nonexempt material shall be separated from the exempt material and released.

Source: Source: Department of Justice "Freedom of Information Guide." http://www.usdoj.gov/oip/foi-act.htm and http://www.usdoj.gov/oip/litigation.htm#reasonably

**Select Agent Sensitive Information**

The portion of the National Laboratory Registration and Select Agent Program information that has been determined by the HHS Original Classification Authority to be sensitive but unclassified and is prohibited from public disclosure by Public Law 107-188, Public Health

Security and Bioterrorism Preparedness and Response Act of 2002. See also 42 USC 247d-6b (d).

Source: Centers for Disease Control. "Manual Guide - Information Security CD.C.-02."
Office of Security and Emergency Preparedness "Sensitive But Unclassified Information." 07/22/2005, http://www.fas.org/sgp/othergov/cD.C.-sbu.pdf.

**Semantic Traffic Analyzer**

A software application [installed by National Security Agency's "secret room" inside AT&T's San Francisco switching office] that runs on standard IBM or Dell servers using the Linux operating system. It's renowned within certain circles for its ability to inspect traffic in real time on high-bandwidth pipes, identifying packets of interest as they race by at up to 10 Gbps.

Internet companies can install the analyzers at every entrance and exit point of their networks, at their "cores" or centers, or both. The analyzers communicate with centralized "logic servers" running specialized applications. The combination can keep track of, analyze and record nearly every form of internet communication, whether e-mail, instant message, video streams or VOIP phone calls that cross the network.

Source: Robert Poe. "The Ultimate Net Monitoring Tool." *Wired* May 17, 2006., http://www.wired.com/news/technology/0,70914-0.html and Narus http://www.narus.com/

**Senior Official of the Intelligence Community (SOIC)**

The head of an agency, office, bureau, other intelligence element as identified in Section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and Section 3.4(f) (1 through 6) of Executive Order 12333.

Source: Director of Central Intelligence "Directive 1/7 Security Controls on the Dissemination of Intelligence Information." June 30, 1998, http://www.fas.org/irp/offdocs/D.C.id1-7.html

**Sensitive**

1. Information pertaining to significant law enforcement cases currently under investigation;

Corruption (police or other government officials), or other sensitive information;
Informant identification information; and Criminal intelligence reports which require strict dissemination and release criteria.

Source: David L. Carter. Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies. Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404

2. Requiring special protection from disclosure that could cause embarrassment, compromise, or threat to the security of the sponsoring power. May be applied to an agency, installation, person, position, document, material, or activity.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Sensitive But Unclassified Information**

1. "An overarching term: Loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled to under Section 552a of Title 5 as amended, but which has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the defense of national interest or foreign policy."

The following Department of Homeland Security information categories fall under SBU:
For Official Use Only (FOUO)
Official Use Only (OUO)
Sensitive Homeland Security Information (SHSI)
Limited Official Use (LOU)
Law Enforcement Sensitive (LES)
Safeguarding Information (SGI)
Unclassified Nuclear Information (UCNI)
Any other information agencies use to categorize information as sensitive but unclassified.

Source: FAS. "Department of Homeland Security Non-Disclosure Agreement."
http://www.fas.org/sgp/othergov/dhs-nda.pdf

2. SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure ser forth under Section 552 and 552a of Title 5 U.S.C., the Freedom of Information Act and the Privacy Act. SBU information includes, but is not limited to:

(1)Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and
(2)Information offered under conditions of confidentiality which arises in the courser of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from advice and counsel of subordinates to policy makers.

Source: United States. Department of State. Volume 12 FAM 540. "Sensitive But Unclassified Information (SBU)." http://www.state.gov/m/a/dir/regs/

3. Sensitive But Unclassified" (formerly "Limited Official Use") information. Sensitive But Unclassified (SBU) information is information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act. Before 26 May 1995, this information was designated and marked "Limited Official Use (LOU)." The LOU designation will no longer be used.

Source: DoD. DOD 5200.1-R Information Security Program. Appendix C, http://fas.org/irp/doddir/dod/5200-1r/appendix_c.htm

4. In response to technological developments in cryptography, computer systems security, on September 17, 1984, Ronald Reagan signed National Security Decision Directive 145 (NSDD-145). The NSDD-145 authorized NSA to develop means to protect "unclassified sensitive" information. NSDD-145 permitted NSA to control the dissemination of government, government-derived, and even non-government information that might adversely affect "national security;" some interpretations of the Directive include broad definitions of information that should be protected such as "all information" included in scientific and technology [transfer] that resides in public libraries and databases such as Dialog, Lexis-Nexis and other commercial products. According to the Electronic Privacy Information Center (EPIC), this was "the first time in its thirty-two year history, the NSA was assigned responsibilities outside its traditional foreign eavesdropping and military and diplomatic communications security roles."[59]

Source: "Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection (PCCIP)," Electronic Privacy Information Center Washington, D.C. 1998, http://epic.org/reports/epic-cip.html , and U.S. National Commission on Libraries and Information Science (NCLIS). *Hearing on Sensitive But Not Classified Information*. May 28, 1987. SUDOC: Y 3.L 61:2 H 35

5. Unclassified information may only be shared with individuals who are determined to have a "need to know" it. Furthermore, DHS employees and contractors must sign a special Non-Disclosure Agreement before receiving access to unclassified FOUO information. DHS directive (MD 11042)

---

[59] NSDD-145 states: "This Directive establishes initial objectives of policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation." ; at (10) "Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information. " FAS, Presidential Directives and Executives Orders, http://www.fas.org/irp/offdocs/nsdd145.htm

Source: "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," May 11, 2004, (obtained by *Secrecy News* through the Freedom of Information Act.)
and http://www.fas.org/sgp/othergov/dhs-sbu.html ; superseded by MD 11042.1, January 5, 2005.

6. The "sensitive but unclassified" designation is applied to unclassified information that may be exempt from mandatory release to the public under FOIA. (For the nine FOIA exemptions, see the FOIA definition in this section.) SBU is the formal designation for information that, by law or regulation, requires some form of protection but is outside the formal system of classification, in accordance with Executive Order 12958, as amended.

Source: Centers for Disease Control. "Sensitive But Unclassified Information."
February 2006, http://www.fas.org/sgp/othergov/cD.C.-sbu-2006.html

7. In addition to information that could reasonably be expected to assist in the development or use of weapons of mass destruction, which should be classified or reclassified as described in Parts I and II above, departments and agencies maintain and control sensitive information related to America's homeland security that might not meet one or more of the standards for classification set forth in Part 1 of Executive Order 12958. The need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information.

Source: Andrew Card. ("The Card Memo") "Guidance on Homeland Security Information Issued." March 21, 2002, , [See the Wayback Machine, http://tinyurl.com/ycvby6e ]

8. Guideline 3 - Standardize Procedures for Sensitive But Unclassified Information To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, procedures and standards for designating, marking, and handling SBU information (collectively "SBU procedures") must be standardized across the Federal Government. SBU procedures must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State, local, and tribal governments, law enforcement agencies, and private sector entities. This effort must be consistent with Executive Orders 13311 and 13388, section 892 of the Homeland Security Act of 2002, section 1016 of IRTPA, section 102A of the National Security Act of 1947, the Freedom of Information Act, the Privacy Act of 1974, and other applicable laws and executive orders and directives.

(i) Within 90 days after the date of this memorandum, each executive department and agency will conduct an inventory of its SBU procedures, determine the underlying authority for each entry in the inventory, and provide an assessment of the effectiveness of its existing SBU

procedures. The results of each inventory shall be reported to the DNI, who shall provide the compiled results to the Secretary of Homeland Security and the Attorney General.

Source: Whitehouse Press Release. "Guidelines and Requirements in Support of the Information Sharing Environment." December 16, 2005, http://www.fas.org/sgp/news/2005/12/wh121605-memo.html and FAS. *Secrecy News* December 20, 2005, http://www.fas.org/sgp/news/secrecy/2005/12/122005.html

9. DHS Form 11000-6, Sensitive But Unclassified Information Nondisclosure Agreement (NDA), as a condition of access to such information. Others not contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager.
The revised DHS policy invalidates previously signed NDAs. Pursuant to the revised policy, DHS Office of Security will develop and implement an education and awareness program for the safeguarding of SBU information. Once the program is developed and appropriate notifications are provided, all employees will participate in classroom or computer-based training sessions designed to educate employees on what constitutes SBU information.

Source: Department of Homeland Security Management Directive 11042 http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf; DHS Management Directive 11042.1, revised January 6, 2005, http://www.fas.org/sgp/othergov/dhs20050111.pdf and FAS. *Secrecy News* January 12, 2005. http://www.fas.org/sgp/news/secrecy/2005/01/011205.html

10. Using targeted FOIA requests and research, the Archive gathered data on the information protection policies of 37 major agencies and components. Of the agencies and components analyzed, only 8 of 37 (or 22%) have policies that are authorized by *statute or regulation* while the majority (24 out of 37, or 65%) follow information protection policies that were generated internally, for example by directive or other informal guidance. Eleven agencies reported no policy regarding sensitive unclassified information or provided no documents responsive to the Archive's request.

Among the agencies and components that together handle the vast majority of FOIA requests in the federal government, 28 distinct policies for protection of sensitive unclassified information exist: some policies conflate information safeguarding markings with FOIA exemptions and some include definitions for protected information ranging from very broad or vague to extremely focused or limited.

Source: National Security Archive. PSEUDO-SECRETS: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information. March 2006. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB183/SBU%20Report%20final.pdf, and Genevieve J. Knezo. "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information." *CRS Report to Congress* February 15, 2006, http://www.fas.org/sgp/crs/secrecy/RL33303.pdf

11. GAO reviewed 56 different sensitive but unclassified designations (16 of which belong to one agency – **NOTE: SBU categories by agency is included in the report**) to protect information that they deem critical to their missions—for example, sensitive law or drug enforcement information or controlled nuclear information. For most designations there are no governmentwide policies or procedures that describe the basis on which an agency should assign a given designation and ensure that it will be used consistently from one agency to another. Without such policies, each agency determines what designations and associated policies to apply to the sensitive information it develops or shares. More than half the agencies reported challenges in sharing such information.

Source: GAO. *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information.* GAO-06-385, March 2006, http://www.gao.gov/new.items/d06385.pdf

Also see *Secrecy News* January 16, 2008, "Pentagon Tackles Control on Unclassified Information" http://www.fas.org/blog/secrecy/2008/01/pentagon_tackles_controls_on_u.html

12. SBU information is currently shared according to an ungoverned body of policies and practices that confuse both its producers and users. Across the Federal Government today more than 100 unique markings and over 130 different labeling or handling processes and procedures are used for SBU information. The result is an unmanageable collection of SBU sharing practices that impede the proper flow of information between Federal, SLT, and private sector partners. This is a national concern because the terrorist threat to the nation requires that many communities of interest, at different levels of government, share this vital but sensitive information.

Although the President's approval of the new CUI framework means that, for the ISE, all SBU information is now CUI, in this Report we continue to use the terms interchangeably because of the deep historical roots of the term "SBU." Over time, however, the term CUI will replace SBU.

Source: ISE, *Annual Report to Congress on the Information Sharing Environment* 2008, http://www.fas.org/irp/agency/ise/2008report.pdf

13. Although the CUI Framework is intended to improve the sharing of only terrorism-related information, the Task Force concluded that a single, standardized framework for marking, safeguarding, and disseminating all Executive Branch SBU is required to further the goals of:

- standardizing currently disparate terminology and procedures (represented by over 107 distinct SBU regimes);

- facilitating information-sharing through the promulgation of common and understandable rules for information protection and dissemination;
- and enhancing government transparency through policies and training that clarify the standards for protecting information within the Framework. (p. viii)

Source: Report and Recommendations of the Presidential Task Force on Controlled Unclassified Information, August 25, 2009, http://www.dhs.gov/xlibrary/assets/cui_task_force_rpt.pdf
**NOTE:** A comprehensive list of SBU Markings Currently in Use is located in Appendix 2.

### Sensitive by Aggregation

Refers to the fact that information on one site may seem unimportant, but when combined with information from other web sites, it may form a larger and more complete picture that was neither intended nor desired. Similarly, the compilation of a large amount of information together on one site may increase the sensitivity of that information and make it more likely that site will be accessed by those seeking information that can be used against the government.

Source: Centers for Disease Control. "Manual Guide - Information Security CD.C.-02."
Office of Security and Emergency Preparedness "Sensitive But Unclassified Information." Part B. 07/22/2005, http://www.fas.org/sgp/othergov/cD.C.-sbu.pdf.

### Sensitive Compartmented Information (SCI)

***See Codewords***

1. Reagan National Security Decision Directive 84, "Safeguarding National Security Information" (March 11, 1983) directed "all persons with access to Sensitive Compartmented Information (SCI) shall be required to sign a nondisclosure agreement as a condition of access to SCI and other classified information, and that this particular agreement must include a provision for prepublication review of writing for public consumption to assure deletion of SCI and other classified information."

Source: FAS. National Security Decision Directives, http://www.fas.org/irp/offdocs/nsdd/nsdd-084.htm

2. Further restricts access to the most sensitive information by imposing special controls, or "compartments" of information for a specific function. SCI is given code words, and colors. Elite groups, who are subject to more stringent background checks, are given the code words to access each compartment. Classified Intelligence Information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

Source: Defense Security Service. National Industrial Security Program,

http://www.fas.org/sgp/library/nispom/chap_09.htm, and 50 U.S.C.15 Subchapter VI § 435a, http://www.gpoaccess.gov/uscode/browse.html

3. Classified Information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director or Central Intelligence. This term does not include Restricted Data as defined in Section II, Public Law 83-703, and Atomic Energy Act of 21954 as amended.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

4. All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (These controls are over and above the provisions of DOD 5200.1-R, Information Security Program Regulation.)

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

5. Special access programs and sensitive compartmented information that forms its most highly guarded subset are the ultimate in security confusion. They represent an ultrasecret classification defined by a set of codes and markings imposed by individual federal agencies on existing classification categories…these new levels of above top secret have confused even political leaders.

Source: Herbert N. Foerstel. *Secret Science: Federal Control of American Science and Technology.* Westport, CT: Praeger, 1993.

6. SCI refers to information that is derived from intelligence sources and methods. It is protected under procedures established by the Director of Central Intelligence.

Source: FAS. *Secrecy News* September 4, 2001, http://www.fas.org/sgp/news/secrecy/2001/09/090401.html

**Types of SCI**:

- **Covered Classified Material**

Any material classified at the Sensitive Compartmentalized Information (SCI) level.

Source: War and National Defense. 50 U.S.C. 15 Subchapter VI § 435a, http://www.gpoaccess.gov/uscode/browse.html

- **Non-Accountable SCI**

SCI (sensitive compartmented information) that does not require document accountability.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

- **TK**

Unclassified term to describe a type of SCI.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

**Sensitive Compartmented Information (SCI) Control Systems/Codewords**
An SCI Control System is the system of procedural protective mechanisms used to regulate or guide each program established by the D.C.I as SCI. A Control System provides the ability to exercise restraint, direction, or influence over or provide that degree of access control or physical protection necessary to regulate, handle or manage information or items within an approved program.

The three SCI Control Systems included in the register are: BYE, COMINT and TALENT KEYHOLE.

Source: DoD. "Intelligence Community Classification and Control Markings Implementation," http://www.fas.org/sgp/othergov/icmarkings.ppt

**Sensitive Compartmented Information Facility (SCIF)**
1. Accredited area, room, or group of rooms, buildings, or installation where SCI may be stored, used, discussed, and /or processed.

Source: Committee for National Security Systems (CNSS). Instruction 4009. National Information Assurance Glossary, June, 2006. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

2. An accredited area, room, group of rooms, or installation where sensitive compartmented information (SCI) may be stored, used, discussed, and/or electronically processed. Sensitive compartmented information facility (SCIF) procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. Also called SCIF. See also sensitive compartmented information.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Sensitive Homeland Security Information (SHSI)**

***See Homeland Security Information, Sensitive But Unclassified***

1. Section 392 of the Homeland Security Act of 2002 required the President to prescribe and implement procedures by which agencies would "identify and safeguard homeland security information that is sensitive but unclassified." A U.S. Government official who spoke to Secrecy News on condition of anonymity stated that a government-wide policy on protecting SHSI "has been periodically discussed, pushed close to some action, and then sent back for further study. There are a dozen hard and fast deadlines that have been missed on this whole subject. I think it's fair to say it's dead. The concept is not dead but it's highly unlikely anything will come of it."

Because Congress failed to define the statutory meaning of "sensitive," critics including the Federation of American Scientists were concerned that the establishment of the "Sensitive Homeland Security Information" (SHSI) category was an invitation to formalize the indiscriminate withholding of information. Meanwhile, however, he [the official] said that a separate interagency initiative was underway to define and regulate the even broader category of "sensitive but unclassified" information. Given that agencies were unable to reach consensus on the definition of terrorism-related SHSI, it will be "exponentially more difficult" to come to agreement on the vastly larger and more amorphous domain of "sensitive but unclassified" information, he said.

Source: FAS Project on Government Secrecy. "The Demise of Sensitive Homeland Security Info." No. 113 December 12, 2005, http://www.fas.org/sgp/news/secrecy/2005/12/121205.html

2. Established in the Homeland Security Act of 2002, which "calls for us to identify and safeguard homeland security information that is sensitive, but unclassified." The regulations governing this category have not been completed.

Source: Remarks by Secretary Ridge to the Association of American Universities http://www.dhs.gov/xnews/speeches/speech_0104.shtm ; Alice R. Buckhalter, John Gibbs, and Marieke Lewis. "Laws and Regulation Governing the Protection of Sensitive But Unclassified Information." Federal Research Division, Library of Congress. September 2004, http://www.loc.gov/rr/frd/pdf-files/sbu.pdf ; Andrew Card. ("The Card Memo") "Guidance on Homeland Security Information Issued," March 21, 2002, [See the Wayback Machine, http://web.archive.org/web/20080306140939/http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm ]

3. Rep. Sabo, the top Democrat on the Homeland Security Subcommittee, offered an amendment to the Department of Homeland Security FY06 funding bill, requiring DHS to clarify "SSI" policy and procedure, including which staff may appropriately have designation

authority. The amendment also withholds $10 million until the Department documents and justifies its use. The amendment was approved by the Appropriations Committee.

Source: Press Release "Sabo Amendment Addresses Abuse of "SSI" Designation within the DHS." May 10, 2005, http://www.fas.org/sgp/news/2005/05/sabo051005.html

**Sensitive Information**

1. a. The Computer Security Act of 1987 established requirements for protection of certain information in Federal Government automated information systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

b. Two aspects of this definition deserve attention. First, the Act applies only to unclassified information that deserves protection. Second, unlike most other programs for protection of information, the Act is concerned with protecting the availability and integrity, as well as the confidentiality of information. Much of the information which fits the Act's definition of "sensitive" falls within the other categories of information discussed in this Appendix. Some does not.

Source: DoD. DOD 5200.1-R Information Security Program. Appendix C, http://fas.org/irp/doddir/dod/5200-1r/appendix_c.htm

2. Classified or Sensitive Unclassified Information.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

3. Any information, the loss, or misuse, or unauthorized access to which would or could adversely affect the organizational and/or national interest but which does not meet criteria specified in DoD 5200.1R (reference (c)).

Source: Department of Defense. DoD 5200.1-M. Acquisition Systems Protection Program. March 1994, http://www.dtic.mil/whs/directives/corres/pdf/52001m_0394/p52001m.pdf

**Sensitive Intelligence Information**

Such intelligence information, the unauthorized disclosure of which would lead to counteraction,

(1) Jeopardizing the continued productivity of intelligence sources or methods which provide intelligence vital to the national security; or (2) Offsetting the value of intelligence vital to the national security.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/

**Sensitive Position**

Any position within the Department of the Army the occupant of which could bring about by virtue of the nature of the position a material adverse effect on the national security. Such positions include any duty or responsibility which require access to top secret, secret or confidential information or material, or any other position so designated by the Secretary of the Army or his designee.

Source: Department of the Army Dictionary of United States Army Terms. Army Regulation 310-25. October,1983, http://www.fas.org/irp/doddir/army/ar310-25.pdf

**Sensitive Security Information (SSI) (1- TSA)**

The Transportation Safety Administration, created in 2001 by the Aviation and Transportation Security Act, November 19, 2001 (P.L. 107-71), has authority to withhold certain information from public disclosure as well as develop regulations regarding the establishment of regulations regarding SSI. The *Code of Federal Regulations* outlines what constitutes SSI: In accordance with 49 U.S.C. 114(s), SSI is

information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would--

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to the security of transportation. [continued]

Sollenberger (6: 2004b) points out, SSI is "born protected." That is, SSI regulations "prohibit TSA from making available to the public any transportation information 'obtained or developed during security activities, or research and development activities.' (see number 15, above). Classifying NSI (national security information) requires government officials to determine, pursuant to EO 12958 "that the document contains national security, intelligence, or foreign relations information "that qualifies as being withheld from public disclosure.

2. Commenting on the posting of "an outdated, unclassified version of a Standard Operating Procedures document…to the Federal Business Opportunities Web site" (TSA), FAS remarked that "…existing legal authorities cannot easily be used to compel the removal of such records from public websites, and that any attempt to do so would likely be counterproductive, and would itself do damage to press freedom and other societal values."

Source: TSA, "TSA Statement on Posting of Operations Document," http://www.tsa.gov/press/happenings/standard_operating_procedures.shtm and FAS, "Disclosure of TSA Manual Stirs Leak Anxiety," *Secrecy News* December 10, 2009, http://www.fas.org/blog/secrecy/2009/12/leak_anxiety.html

**10.25.2006**: The Homeland Security Appropriations Act [2007] include provisions that documents categorized as "sensitive security information" (SSI) be released after three years.

Source: 49 CFR 1520.5. Transportation Security Administration, Department of Homeland Security. http://www.gpoaccess.gov/cfr/index.html; Mitchel Sollenberger. "Sensitive Security Information (SSI) and Transportation Security: Background and Controversies." *CRS Report for Congress* February 5, 2004a, http://www.firstamendmentcenter.org/pdf/CRS.security1.pdf ; "Sensitive Security Information and Transportation Security: Issues and Congressional Options." *CRS Report for Congress* June 9, 2004b, http://www.fas.org/sgp/crs/RL32425.pdf ; GAO-05-677. "Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information." June 2005, http://www.gao.gov/highlights/d05677high.pdf; Steven Aftergood. "The Secrets of Flight." *Slate* November 18, 2004, http://slate.msn.com/id/2109922/ ; Harold Relyea. "Security Classified and Controlled Information: History, Status, and Emerging Management Issues." *CRS Report to Congress* June 26, 2006, http://www.fas.org/sgp/crs/secrecy/RL33494.pdf , and Gina Marie Stevens and Todd B. Tatelman. "Protection of Security-Related Information." *CRS Report for Congress* September 27, 2006, http://www.fas.org/sgp/crs/secrecy/RL33670.pdf

2. The conferees are concerned that because of insufficient management controls, information that should be in the public domain may be unnecessarily withheld from public scrutiny. The conferees require the Secretary to ensure that each appropriate office has an official with the clear authority to designate documents as SSI and to provide clear guidance as to what is SSI material and what is not. Designation means an original determination made by a limited number of appointed officials pursuant to 49 CFR Sec. 1520.5(b (1)-(16)). The conferees direct the Secretary to report to the Committees not later than January 3, 2006, the titles of all documents that are designated by DHS as SSI in their entirety during the period beginning October 1, 2005, and ending December 31, 2005, and a full-year report each year thereafter.

Source: House of Representatives. Conference Report on H.R. 2360, Department of Homeland Security Appropriations Act, 2006. H. Report 109-241. http://www.fas.org/sgp/congress/2005/dhs-ssi.html and Thomas http://thomas.loc.gov/cgi-bin/query/F?r109:1:./temp/~r1093OrAas:e111888:

**Sensitive Security Information (SSI) (2 - USDA)**

***See For Official Use Only, Sensitive But Unclassified***

Unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity; and which describes, discusses, or reflects:

1. The ability of any element of the critical infrastructure of the United States to resist intrusion, interference, compromise, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law; harms interstate, international commerce of the United States; or, threatens public health or safety;
2. Any currently viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including, but not limited to vulnerability assessment, security testing, risk evaluation, risk-management planning, or risk audit;
3. Any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States, specifically including but not limited to the repair, recovery, redesign, reconstruction, relocation, insurance, and continuity of operations of any element;
4. The following categories are provided for illustration purposes only as examples of the types of information (regardless of format) that may be categorized as SSI:
    1. Physical security status of USDA laboratories, research centers, field facilities, etc., which may also contain vulnerabilities;
    2. Investigative and analytical materials concerning information about physical security at USDA facilities such as the above-named facilities;
    3. Information that could result in physical risk to individuals;
    4. Information that could result in serious damage to critical facilities and/or infrastructures;
    5. Cyber Security Information, which includes, but is not limited to
        a. Network Drawings or Plans
        b. Program and System Security Plans
        c. Mission Critical and Sensitive Information Technology (IT) Systems and Applications
        d. Capital Planning and Investment Control Data (I-TIPS)
        e. IT Configuration Management Data and Libraries
        f. IT Restricted Space (Drawings, Plans and Equipment Specifications as well as actual space)
        g. Incident and Vulnerability Reports
        h. Risk Assessment Reports, Checklists, Trusted Facilities Manual and Security Users Guide
        i. Cyber Security Policy Guidance and Manual Chapters

USDA refers to unclassified sensitive information as "Sensitive Security Information" (SSI), and says “basically, it's to be treated the same as "Sensitive But Unclassified Information" or "For Official Use Only Information.”

Source: U.S. Department of Agriculture (U.S.D.A.). DR 3440-2 “Control and Protection of Sensitive Security Information.” January 30, 2003, http://www.da.usda.gov/pdsd/ssi.htm, and Harold Relyea. “Security Classified and Controlled Information: History, Status, and Emerging Management Issues.” *CRS Report to Congress* June 26, 2006, http://www.fas.org/sgp/crs/secrecy/RL33494.pdf

2. The conferees are concerned that because of insufficient management controls, information that should be in the public domain may be unnecessarily withheld from public scrutiny. The conferees require the Secretary to ensure that each appropriate office has an official with the clear authority to designate documents as SSI and to provide clear guidance as to what is SSI material and what is not. Designation means an original determination made by a limited number of appointed officials pursuant to 49 CFR Sec. 1520.5(b (1)-(16)). The conferees direct the Secretary to report to the Committees not later than January 3, 2006, the titles of all documents that are designated by DHS as SSI in their entirety during the period beginning October 1, 2005, and ending December 31, 2005, and a full-year report each year thereafter.

Source: House of Representatives. Conference Report on H.R. 2360, Department of Homeland Security Appropriations Act, 2006. H. Report 109-241, http://www.fas.org/sgp/congress/2005/dhs-ssi.html and Thomas http://thomas.loc.gov/cgi-bin/query/F?r109:1:./temp/~r1093OrAas:e111888:

**Sensitive Security Information (3-DHS)**
In an attempt to limit unnecessary controls on unclassified information, Congress last year required the Department of Homeland Security to identify by title all DHS documents that were marked as "Sensitive Security Information" (SSI) that may not be publicly disclosed. In response, the first DHS report to Congress listed approximately one thousand titles that had been marked as SSI between October 1 and December 31, 2005.

A copy of that report has just been released with minor redactions in response to a Freedom of Information Act request from the Federation of American Scientists.

Source: *Secrecy News*, “DHS lists ‘sensitive security information titles,’” "Department of Homeland Security Documents Designated in Their Entirety as Sensitive Security Information (SSI), October 1 Thru December 31, 2005,” http://www.fas.org/sgp/othergov/dhs/ssi-titles.pdf

**Sensitive Site Exploitation**
A related series of activities inside a captured sensitive site to exploit personnel documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site or its contents. Also called SSE.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Sensitive Unclassified Information**

1. Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U.S. Government. Governmental interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law-enforcement information, as well as the privacy or confidentially of personal or commercial proprietary information provided by the U.S. Government by its citizens.

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995. http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. Information which, either alone or in the aggregate, meets any of the following criteria and is deemed sensitive by the Department of State, and must be protected in accordance with the magnitude of its loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction of the data:

Medical, personnel, financial, investigative or any other information the release of which would result in substantial harm, embarrassment, inconvenience, or unfair treatment to the Department or any individual on whom the information is maintained, such as information protected by 5 U.S.C. 522a;

Information relating to the issuance or refusal of visas or permits to enter the United States, as stated in Section 222, 8 U.S.C. 1202;

Information which may jeopardize the physical safety of Department facilities, personnel and their dependents, as well as U.S. citizens abroad;

Proprietary, trade secrets, commercial or financial information the release of which would place the company or individual on whom the information is maintained at a competitive disadvantage;

Information the release of which would have a negative effect on foreign policy or relations

Information relating to official travel to locations deemed to have a terrorist threat;

Information considered mission-critical to an office or organization, but which is not national security information; and

Information which could be manipulated to commit fraud.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12 FAM 090, "Definitions of Diplomatic Security Terms." November 13, 2003. http://www.state.gov/m/a/dir/regs/

**Sentiment Analysis**

1. The evaluation of the sentiment – typically positive or negative – of the text based on the usage of language. Determining the sentiment (general tone) of a document based on the application of computational linguistics algorithms.

Source: FAST http://www.fastsearch.com/glossary.aspx?m=48&amid=389

2. A consortium of major universities, using Homeland Security Department money, is developing software that would let the government monitor negative opinions of the United States or its leaders in newspapers and other publications overseas. Such a "sentiment analysis" is intended to identify potential threats to the nation, security officials said.

Source: Eric Lipton, Software Being Developed to Monitor Opinions of U.S., *New York Times* October 4, 2006.

3. CS professors Claire Cardie and Lillian Lee are working on sentiment-analysis technologies for extracting and summarizing *opinions* from unstructured human-authored documents. They envision systems that (a) find reviews, editorials, and other expressions of opinion on the Web and (b) create condensed versions of the material or graphical summaries of the overall consensus

Source: Cornell University. "Sentiment Analysis."

**Server in the Sky**

The FBI told the Guardian: "Server in the Sky is an FBI initiative designed to foster the advanced search and exchange of biometric information on a global scale. While it is currently in the concept and design stages, once complete it will provide a technical forum for member nations to submit biometric search requests to other nations. It will maintain a core holding of the world's 'worst of the worst' individuals. Any identification of these people will be sent as a priority message to the requesting nation."

Source: Owen Bowcott, "FBI wants instant access to British identity data," *The Guardian* January 15, 2008, http://www.guardian.co.uk/uk/2008/jan/15/world.ukcrimeR and ichard Koman, "'Server in the Sky' FBI international biometric db planned," *ZDNe*t January 14, 2008, http://government.zdnet.com/?p=3605

**Seven Member Rule**

1. An Executive agency, on request of the Committee on Government Operations of the House of Representatives, or of any seven members thereof, or on request of the Committee on Governmental Affairs of the Senate, or any five members thereof, shall

submit any information requested of it relating to any matter within the jurisdiction of the committee.

Source: 5 U.S.C. § 2954. "Information to Committees of Congress on Request." http://www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00002954----000-.html

2. As a matter of legal interpretation, the Department of Justice has taken the position that the Seven Member Rule does not entitle members of the Government Reform Committee to information from the executive branch. As a matter of practice, however, federal agencies have commonly complied with requests under the Seven Member Rule.

The Bush Administration, however, has resisted providing members information under the Seven Member Rule, forcing Committee members to initiate litigation on two separate occasions to enforce their rights. The first case involved census records. On April 6, 2001, eighteen members of the Government Reform Committee used the Seven Member Rule to request the adjusted data for the 2000 Decennial Census from the department of Commerce. The request was made because the Department had prepared both an unadjusted data set and a data set adjusted for sampling errors, but had only released the unadjusted data. The Bush Administration rejected the request.

Source: U.S. House of Representatives. Committee on Government Reform. "Secrecy in the Bush Administration." September 14, 2004. 82-83, http://democrats.reform.house.gov/features/secrecy_report/pdf/pdf_secrecy_report.pdf

**Shield Laws**

Absent a statutory or constitutional recognition of journalists' privilege, a reporter may be compelled to testify in legal, administrative, or other governmental proceedings. Thirty-three states and the District of Columbia have recognized a journalists' privilege through enactment of press "shield laws," which protect the relationship between reporters, their source, and sometimes, the information that may be communicated in that relationship.1 Another 16 states have recognized a journalists' privilege through court decisions; Wyoming is the only state that has no legislatively or judicially adopted journalists' privilege. The journalists' privilege is distinct from other recognized privileges in that it vests only with the journalist, not with the source of the information.

Source: Henry Cohen," Journalists' Privilege to Withhold Information in Judicial and Other Proceedings: State Shield Statutes," CRS *Report to Congress* June 27, 2007, http://www.fas.org/sgp/crs/secrecy/RL32806.pdf

**SIGMA Categories**

***See Classification Markings / Control Markings, Formerly Restricted Data, Restricted Data***

1. Within the Restricted Data and Formerly Restricted Data categories, SIGMA designates degrees of access to information concerning the design, manufacture, or utilization of nuclear weapons or nuclear explosive devices. There are 16 categories of SIGMA [see http://www.fas.org/sgp/othergov/doe/sigmas.html]

Source: Department of Energy. Office of Security Affairs. Office of Safeguards and Security. "Safeguards and Security Glossary of Terms." December 18, 1995, http://www.directives.doe.gov/pdfs/doe/doetext/neword/470/m4704-7.pdf

2. Sigma 16, which would entail increased protection for certain information, emerged from former Energy Secretary Hazel O'Leary's "higher fences" initiative back in 1997 and even earlier.

Currently, information on the design, manufacture and utilization of nuclear weapons is broken down into 15 so-called Sigma categories. The present definitions of these categories, as well as that of the pending Sigma 16, may be found here: http://www.fas.org/sgp/othergov/doe/sigmas.html

Source: FAS. *Secrecy News* September 4, 2001, http://www.fas.org/sgp/news/secrecy/2001/09/090401.html

3. Sigmas are categories of information related to the design, manufacture, or utilization of atomic weapons or nuclear explosive devices that require different or more stringent protection. Sigma 16 will be a new category comprised of documents containing 1. nuclear weapons design specifications that would permit the reproduction and function of the weapons, and 2. aggregations of design information that provide comprehensive insight into nuclear weapons capability, vulnerability, or design philosophies.

Source: United States. General Accounting Office. *Nuclear Security: DOE Needs to Improve Control over Classified Information.* Washington, D.C.: U.S. General Accounting Office, 2001, http://www.gao.gov/new.items/d01806.pdf

### Situational Understanding

The product of applying analysis and judgment to relevant information to determine the relationships among the mission variables to facilitate decisionmaking. (FM 3-0

Source: Department of the Army, "Knowledge Management Section," U.S. Army Field Manual 6-01.1, August 29, 2008, http://www.fas.org/irp/doddir/army/fm6-01-1.pdf

### Smith-Mundt Act of 1948

***See Bureau of International Information Programs (IIP), Counter-Information Team, Information Exploitation, Propaganda, Public Diplomacy***

1. The Smith-Mundt Act of 1948 n2 is a key statute outlining the global mission of U.S. propaganda abroad and limitations on distribution of U.S. propaganda at home.

The Smith-Mundt Act established exchange of students, professors, books and educational materials between the United States and other countries. The act also authorized the federal government -- specifically, the State Department -- to employ its own agencies and private organizations to "disseminate abroad . . . information about the United States, its people, and its policies, through press, publications, radio, motion pictures, and other information media, and through information centers and instructors abroad." This effort was necessary, Congress asserted, because America had shortsightedly failed to systematically promote itself to other nations, and by 1948 the United States was engaged in a massive and bitter propaganda war with the Soviet Union for the hearts and minds of the world.

Source: Allen W. Palmer and Edward L. Carter. "The Smith-Mundt Act's Ban on Domestic Propaganda: An Analysis of the Cold War Statute Limiting Access to Public Diplomacy." *Communications Law and Policy* 11 no.1 (Winter 2006): 1-34.

2. Ban on domestic activities by United States Information Agency: Except as provided in section 1461 of this title and this section, no funds authorized to be appropriated to the United States Information Agency shall be used to influence public opinion in the United States, and no program material prepared by the United States Information Agency shall be distributed within the United States. This section shall not apply to programs carried out pursuant to the Mutual Educational and Cultural Exchange Act of 1961 (22 U.S.C. 2451 et seq.). The provisions of this section shall not prohibit the United States Information Agency from responding to inquiries from members of the public about its operations, policies, or programs [22 U.S.C. CHAPTER 18 > SUBCHAPTER V > § 1461-1a]

Source: U.S. Information and Educational Exchange Act of 1948 ("Smith-Mundt Act of 1948," PL 80-402, 22 U.S.C. 1461); National Security Archive. "Rumsfeld's Roadmap to Propaganda." January 26, 2006. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/index.htm; Pub. L. 108-458, U.S.C VII, § 7108, Dec. 17, 2004, 118 Stat. 3790,

### Social Malware

The combination of well-written malware with well-designed email lures, which we call social malware... (p.3)

But the industrialisation of online crime over the past five years means that capably-written malware, which will not be detected by anti-virus programs, is now available on the market. All an attacker needs is the social skill and patience to work the malware from one person to another until enough machines have been compromised to complete the mission. What's

more, the `best practice' advice that one sees in the corporate sector comes nowhere even close to preventing such an attack. Thus social malware is unlikely to remain a tool of governments. (p.8)

Source: Shishir Nagaraja and Ross Anderson, "The snooping dragon: social-malware surveillance of the Tibetan movement," March 2009, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf and Information Warfare Monitor, *Tracking GhostNet: Investigating a Cyber Espionage Network*, March 2009, http://www.infowar-monitor.net/

### Social Network Analysis [60]

***See Able Danger, Data Mining***

Social network analysis (SNA) is characterized by a distinct and unique methodology for collecting data, performing statistical analysis, and making visual representations. Such applications can be useful for devising more effective schemes for promoting ideas or exerting influence in organizations. These are certainly important functions, but the relevance of such analysis to counterinsurgency (COIN) primarily deals with explaining how people behave and how that behavior is affected by their relation-
ships. In the past, SNA contributed to the British success in defeating the Malaysian insurgency. More recently in Iraq, it has been used in the calming of the Fallujah region by the U.S. Marine Corps, and in the capture of Saddam Hussein by the 4th Infantry Division.

For an insurgency, a social network is not just a description of who is in the insurgent organization, but a picture of the population, how they are put together, and how they interact with one another. Often, social networks are large, complex, and amorphous. They can be beyond the cognitive limitations of a human analyst.

Source: Department of the Army. Counterinsurgency Final Draft - Not for Implementation. FM 3-24, FMFM 3-24. June 2006 (Final Draft), http://www.fas.org/irp/doddir/army/fm3-24fd.pdf and Paul Marks. "Pentagon sets its sights on social networking websites." June 9, 2006, http://www.newscientist.com/article/mg19025556.200?D.C.MP=NLC

### Society for Worldwide Interbank Financial Telecommunication (SWIFT)

***See Terrorist Finance Tracking Program***

The SWIFT network carries up to 12.7 million messages a day containing instructions on many of the international transfers of money between banks. The messages typically include the names and account numbers of bank customers — from U.S. citizens to major

---

[60] Artist Mark Lombardi's mind mapping/social networking projects illustrating money laundering, terrorism, and the arms trade are early examples of modeling of networks; also see NPR's "The Conspiracy Art of Mark Lombardi," http://www.npr.org/templates/story/story.php?storyId=1487185 , *Mark Lombardi: Global Networks* [New York: Independent Curators International, 2003], and Edward Tufte's "Design of causal diagrams: Barr art chart, Lombardi diagrams, evolutionary trees, Feynman diagrams, timelines," http://www.edwardtufte.com/bboard/q-and-a-fetch-msg?msg_id=0000yO

corporations — who are sending or receiving funds.

Under the program, [the U.S. Department of the ] Treasury issues a new subpoena once a month, and SWIFT turns over huge amounts of electronic financial data, according to Stuart Levey, the department's undersecretary for terrorism and financial intelligence. The administrative subpoenas are issued under authority granted in the 1977 International Emergency Economic Powers Act.

The Belgium Privacy Commission has found that SWIFT did not obey Belgium law when it transferred vast amounts of financial data to the U.S. Treasury Department.

Source: Josh Meyer and Greg Miller. "Terrorist Finance Tracking Program." http://www.commondreams.org/headlines06/0623-06.htm ; SWIFT, http://www.swift.com/index.cfm?item_id=43232; Jennifer K. Elsea and M. Maureen Murphy. "Treasury's Terrorist Finance Program's Access to Information Held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)." *CRS Report to Congress* July 6, 2006, http://www.fas.org/sgp/crs/natsec/RS22469.pdf; Alexi Mostrous and Ian Cobain. "CIA's secret UK bank trawl may be illegal." *The Guardian* August 21, 2006, http://www.guardian.co.uk/terrorism/story/0,,1854813,00.html and EPIC. "Belgium Data Privacy Commission: Summary of the opinion on the transfer of personal data by SCRL SWIFT following the UST (OFAC) subpoenas," http://www.epic.org/redirect/bel_pc_op0906.html - Note - the Belgian link is dead; try this: Privacy International, "Belgian Prime Minister condemns SWIFT data transfers to U.S. as 'illegal'," http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543789

**Source**

1. A person, thing, or activity from which information is obtained.

2. In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes.

3. In interrogation activities, any person who furnishes information, either with or without the knowledge that the information is being used for intelligence purposes. In this context, a controlled source is in the employment or under the control of the intelligence activity and knows that the information is to be used for intelligence purposes. An uncontrolled source is a voluntary contributor of information and may or may not know that the information is to be used for intelligence purposes.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Source Document(s)**

***See Derivative Classification***

1. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

2. A classified document (i.e., memo, letter, scientific report, etc.) other than a classification guide, from which information is extracted for inclusion in another document.

Source: DOE. *Understanding Classification*. Washington, D.C.: U.S. Dept. of Energy, Assistant Secretary for Defense Programs, Office of Classification, 1987. SUDOC: E 1.15:0007/1

**Sources and Methods**

1. There is no statutory definition of either the phrase or its constituent elements. Therefore, presidents could direct (or the D.C.Is could adopt) a less restrictive interpretation of the provision, by narrowly defining sources and methods that need to be protected.

Source: James X. Dempsey. "The CIA and Secrecy." *A Culture of Secrecy: the Government Versus the People's Right to Know.* Athan G. Theoharis (Ed.), (Lawrence: University Press of Kansas, 1998. 37-59), and Commission on Protecting and Reducing Government Secrecy. Report on the Commission on Protecting and Reducing Government Secrecy, Senate Document 105-2. 1997, http://www.gpo.gov/congress/commissions/secrecy/index.html

2. The CIA charter provides that information concerning the sources and methods of intelligence collection must remain secret. Such information is not available for public disclosure and is redacted (or blacked out) from documents, but significant amounts of analytical or publicly derived information are available.

Source: Central Intelligence Agency. "The Freedom of Information Act, 5 U.S.C. §552." http://www.foia.cia.gov/foia.asp

3. *CIA v. Sims,* a 1985 Supreme Court case that involved a request for information from the Central Intelligence Agency (CIA) regarding a project code-named "MKULTRA." The plaintiffs in Sims made a FOIA request for the names of the approximately eighty institutions and 185 individuals involved in the MKULTRA research. Although the CIA disclosed some names, it invoked FOIA Exemption 3, rather than Exemption 7, to withhold the names of all individual researchers and twenty-one institutions. The Agency relied on a statute that stated "the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure." In deferring to the CIA's judgment that the MKULTRA researchers were "intelligence sources" within the meaning of the statute, the Court held that "the decisions of the Director, who must of course be familiar with the whole picture, as judges are not, are worthy of great deference given the magnitude of the national security interests and potential risks at stake." The majority in

Center for National Security Studies cited this language approvingly, and ruled that decisions of the Justice Department officials in charge of the terrorism investigation are entitled to the same deference.

Source: Bradley Pack. "FOIA Frustration: Access to Government Records Under the Bush Administration." 46 *Ariz. L. Rev.* 815. [notes 154-161] and Sec. 103 (50 U.S.C. 403-3] c (7) National Security Act of 1947 July 26, 1947. (As Amended), http://www.intelligence.gov/0-natsecact_1947.shtml

**Sousveillance**

To view from below.

World Surveillance {Subjectrights} Day is December 24 as proposed by political scientist Ronald Deibert where "ordinary people all over the world will call into question the growing and dehumanizing effects of increased video surveillance, automated face recognition, and Covernment (Corporate+Government) tracking in public places, as well as private places."

Source: CitizenLab
http://www.citizenlab.org/modules.php?op=modload&name=WSD&file=index, Steve Mann, Jason Nolan and Barry Wellman. "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments." Surveillance & Society 1 no. 3(2003): 331-355. http://www.surveillance-and society.org/articles1(3)/sousveillance.pdf and Patrick DiJusto, "Record the Lens That Records You," *Wired* November 28, 2002, http://www.wired.com/culture/lifestyle/news/2002/11/56185

**Special Access Program (SAP)**

1. Any program that imposes need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Examples of such controls include, but are not limited to special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine need to know; or special lists of persons determined to have a need-to-know. Special access controls may be applied to "an extremely sensitive activity requiring special protection from disclosure to prevent significant damage to national security or the reputation or interests of the United States." Any program imposing a need-to-know or access controls beyond those normally provided for access

Source: Army Regulation 380-381, 12 October 1998, section 1-4(6), DoD 5200.1-M, and Army Regulation 380-381, 21 April 2004, http://www.fas.org/irp/DoDdir/army/ar380-381.pdf

2. A sensitive program, approved in writing by a head of agency with original top secret classification authority, that imposes need-to-know and access controls beyond those normally provided for access to confidential, secret, or top secret information. The level of controls is based on the criticality of the program and the assessed hostile

intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

3. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended, http://www.archives.gov/isoo/policy-documents/eo-12958- amendment.html#1.2

4. Any program, which may or may not contain SCI (sensitive compartmented information), imposing a need-to-know and access controls beyond those normally provided for access to CONFIDENTIAL, SECRET AND TOP SECRET information. Such controls may include, but are not limited to, access approval; adjudicative or investigative requirements; special designation of officials authorized to determine need-to-know; or special list or persons determined to have a need-to-know.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

**Special Information Operations (SIO)**
Information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Special Psychological Operations Assessment**
A PSYOP intelligence document that focuses on any of a variety Operations assessment of different subjects pertinent to PSYOP, such as a particular target group, significant social institution, or media analysis. A SPA can serve as an immediate reference for the planning and conduct of PSYOP.

Source: DoD. *Psychological Operations,* FM 3-05.30 MCRP 3-40.6, April 2005, http://www.fas.org/irp/doddir/army/fm3-05-30.pdf

**Split Knowledge**

Separation into data and information into two or more parts, each part constantly kept under control of authorized individuals or teams so no one individual or team will know the whole data.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*, June, 2006. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**Statistical Management Analysis and Reporting Tool System (SMARTS)/SPSS**
***See Data Mining***
Drug Enforcement Agency. Is a query analysis and reporting tool that pulls data from many systems. It allows for statistical analyses of drug cases Drug Enforcement Administration's statistical reporting;
Purpose: Detecting criminal activities or patterns;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Store**
An information management activity: to retain relevant information in any form, usually for orderly, timely retrieval and documentation, until it is needed for exercising command and control.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents

**Stovepipes**
Bureaucratic organizational structure and equities that restrict flexibility to work across organizational lines.

Source: Melissa Boyle Mahle. *Denial and Deception: an Insider's View of the CIA from Iran-Contra to 9/11*. New York: Nation Books.

**Strategic Compression**
The forming of unexpected causal relationships and breaking of expected causal relationships among the tactical, operational, and strategic levels of conflict. Strategic compression accelerates due to the rapidity of information transmission and the lack of understanding of preexisting and emergent trends and social appetites both within the local

area of conflict and within a world-wide audience. As such, the levels of war seem to compress in time and in causal linkages.

Source: U.S. Joint Forces Command, Marines begin Joint Urban Warrior 07, http://www.jfcom.mil/newslink/storyarchive/2007/pa052107.html

**Strategic Communications** [61]

The planning, execution, and assessment of integrated and coordinated US Government themes and messages that advance US interests and policies through a synchronized interagency effort supported by public diplomacy, public affairs, and military information operations in concert with other political, economic, information and military actions.

Source: U.S. Air Force. Public Affairs Operations, Air Force Doctrine Document 2-5.3, June 24, 2005. [See Wayback Machine, http://web.archive.org/web/20061007174450/http://www.e-publishing.af.mil/pubfiles/af/dd/afdd2-5.3/afdd2-5.3.pdf ] Note: DoD 2008 fiscal year budget includes three million dollars for "strategic communication and integration…"

**Strategic Compression**

The forming of unexpected causal relationships and breaking of expected causal relationships among the tactical, operational, and strategic levels of conflict. Strategic compression accelerates due to the rapidity of information transmission and the lack of understanding of preexisting and emergent trends and social appetites both within the local area of conflict and within a world-wide audience. As such, the levels of war seem to compress in time and in causal linkages.

Source: USJFCOM, Joint Urban Warrior 07, http://www.jfcom.mil/newslink/storyarchive/2007/pa052107.html

**Strategic Information Warfare**

***See Cyberwar, Defensive Information Warfare, Direct Information Warfare, Information Warfare, Netwar***

Intersection of information and strategic warfare.

---

[61] The Rendon Group, Inc. was awarded "a $6,400,919 firm-fixed-price contract for Strategic Communications Operation Support" in September, 2005. See DoD Contracts, September 27, 2005, http://www.defenselink.mil/contracts/2005/ct20050927.html & James Bamford (November 17,2005), "The Man Who Sold the War: Meet John Rendon, Bush's General in the Propaganda War," *Rolling Stone* http://www.rollingstone.com/politics/story/8798997/the_man_who_sold_the_war/

Source: Roger C. Molander, et al. "What is Information Warfare?" In *Strategic Information Warfare Rising.* Santa Monica: Rand Corp., 1998, http://www.rand.org/publications/MR/MR964/MR964.pdf/MR964.ch1.pdf

**Strategic Intelligence (SI)**

Examines crime patterns and crime trends for management use in decision making, resource development, resource allocation, and policy planning. Strategic intelligence typically focuses on specific crime types, such as criminal enterprises, drug traffickers, terrorists, or other forms of complex criminality. SI also provides detailed information on a specified type of crime or criminality.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404

**Suspicious Activity Reports (SARs)**

***See Information Sharing Environment (ISE)***

1. The Bank Secrecy Act requires MSBs (Money Services Businesses) to file suspicious activity reports with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). Check cashers and sellers and redeemers of stored value are not required to, but may voluntarily file a SAR.

An MSB must file a SAR when it knows or suspects that: The funds come from illegal activity or disguise funds from illegal activity; the transaction is structured to evade BSA requirements or appears to serve no known business or apparent lawful purpose; or, the MSB is being used to facilitate criminal activity.

Source: Internal Revenue Services, "Suspicious Activity Reports, " http://www.irs.gov/businesses/small/article/0,,id=154555,00.html

2. This year, the LAPD established a department-wide process for gathering, processing, and sharing terrorism-related SARs. Consistent with the ISE-SAR Functional Standard, this process uses e-learning and roll call training to inform officers how to recognize potential terrorist activities while providing standardized reporting codes that facilitate the reporting and review of terrorism related suspicious incidents. LAPD is blending suspicious activity reports with other critical infrastructure and relevant crime data in order to identify patterns and trends that may be indicators of potential threats to locations within the city.

Source: ISE, *Annual Report to Congress on the Information Sharing Environment* 2008, http://www.fas.org/irp/agency/ise/2008report.pdf

**System Accreditation**

The official authorization granted to an information system to process sensitive information in its operational environment based on a comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration and implementation and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 200,. http://www.state.gov/m/a/dir/regs/

**System of Record**

1. From the Privacy Act of 1974, "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Source: 5 U.S.C. 552a (a) (5). The Privacy Act of 1974. EPIC, http://www.epic.org/privacy/1974act/ [kindly supplied by Robert Gellman].

2. The highly technical "system of records" definition is perhaps the single most important Privacy Act concept, because it generally makes coverage under the Act dependent upon the method of retrieval of a record rather than its substantive content. Records must be accessed by the agency by use of a personal identifier. The mere capability or potential for retrieval is not enough. Source: Department of Justice,

Source: "Overview of the Privacy Act of 1974", 2004 Edition, http://www.usdoj.gov/oip/1974definitions.htm#system [kindly supplied by Robert Gellman].

**Systematic Declassification Review**

***See Declassification***

Review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with Title 44, *United States Code*.

Source: ISOO. Executive Order 12958 "Classified National Security Information," Amended. http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2 and Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html

---

**~ T ~**

**Tactical Intelligence (TI)**

***See Intelligence, Intelligence Information***

Seeks to gather and manage diverse information to facilitate a successful prosecution of the intelligence target. TI is also used for specific decision making or problem solving to deal with an immediate situation or crisis.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies*. Dept. of Justice, Office of Community Oriented Policing Services, 2004. http://www.cops.usdoj.gov/default.asp?Item=1404

**Talon Report**

***See Counterintelligence Field Activity (CIFA)***

1. A formatted written record of non-validated threat information.

Source: DoD. "DoD Counterintelligence Collection Reporting." DoD 5240.17. October 26, 2005, http://www.fas.org/irp/doddir/dod/i5240_17.pdf

2. Dec. 15, 2005 - The Defense Department has ordered a review of an intelligence system that compiles information on possible worldwide threats to U.S. military personnel and installations, a senior DoD official said here today.

Some recent news reports allege that the Threat and Local Observation Notice system, known by the acronym TALON, had improperly stored information about some civilian individuals and non-government-affiliated groups on its database.

"It appears as if there may have been things that were left in the database that shouldn't have been left there," DoD spokesman Bryan Whitman told Pentagon reporters.

The TALON system collects and evaluates information about possible threats to U.S. service members and defense civilians at stateside and overseas military installations, Whitman said. Analysts examine the information, he said, to ascertain whether there could be a genuine threat.

The Defense Department announced Dec. 14 that it would conduct a four-point review of the TALON system, Whitman said, that will consist of:

- Examining the TALON reporting system to ensure that it fully complies with DoD procedures and U.S. law;
- Reviewing policies and procedures to make sure that they are being properly applied in respect to any reporting and retention of information on U.S. persons;
- Examining the TALON database to identify any other information that might be improperly stored in the database, and;

- Providing all DoD counterintelligence and intelligence personnel with refresher training concerning the laws, policies and procedures governing the collection, reporting and storage of information related to the warning of potential threats to DoD personnel and facilities.

Source: Gerry J. Gilmore. "DoD Orders Review of Anti-Threat Intel-Gathering System." DefenseLINK News, http://www.defenselink.mil/news/Dec2005/20051215_3672.html

3. The TALON Reporting System is an innovative initiative to document unfiltered and non-validated potential threat information about suspicious activity linked to possible international terrorist threats to DoD personnel and resources that might have otherwise gone unreported. This information is reported by concerned citizens and Department personnel or obtained through information sharing with civilian law enforcement agencies. The program, has been productive.

The review confirmed that TALON Reporting System should be used only to report information regarding possible international terrorist activity, and concluded that all TALON reports should be retained in accordance with DoDD 5240.1-R "Activities of DoD Intelligence Components That Affect United States Persons, " dated December 1982.

Source: Deputy Secretary of Defense Gordon England. "Threats to the Department of Defense." Memo, March 30, 2006, http://www.fas.org/irp/agency/dod/033006talon.pdf

4. DoD's Counterintelligence Field Activity (CIFA) will close the TALON Reporting System effective Sept. 17, 2007, and maintain a record copy of the collected data in accordance with intelligence oversight requirements. To ensure there is a mechanism in place to document and assess potential threats to DoD resources, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs will propose a system to streamline such threat reporting and better meet the Defense department's needs.

In the interim, until this new reporting program is adopted, DoD components will send information concerning force protection threats to the Federal Bureau of Investigation's Guardian reporting system.

Source: Defenselink, http://www.defenselink.mil/releases/release.aspx?releaseid=11251 and TALON was suspended in 2007; see Jeffrey Richelson's *The Pentagon's Counterspies* Electronic Briefing Book @ the National Security Archive, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB230/index.htm

**TANGRAM**

1. Tangram is envisioned as a fully automated, continuously operating, intelligence analysis support system that's capable of configuring itself to achieve a reasonable tradeoff between estimated intelligence value and cost…

This work will be complete September 2010. Air Force Research Laboratory, Rome, N.Y., is the contracting activity. (FA8750-06-C-0208).

See Cryptome has a copy of the TANGRAM "Proposer's Information Packet (PIP)" http://cryptome.info/tangram-intel.htm and DefenseLink, September 25, 2006, http://www.defenselink.mil/Contracts/Contract.aspx?ContractID=3349; also see Shane Harris' "Agency explores new tool to connect intelligence dots." October 20, 2006. http://www.govexec.com/story_page.cfm?articleid=35310&sid=28

2. Seeking to demonstrate the feasibility and intelligence value of a semi-autonomous terrorist threat assessment system concept. Its most immediate objective is to assess the threat likelihood of known threat entities. The simplest of methods would be initiated by a search for information about the specific entity. However, a surveillance and warning system must also provide warnings.

Source: DNI, *Data Mining Report*, February 15, 2008, http://www.fas.org/irp/dni/datamining.pdf

**Tear Line**

***See Write-to-Release***

1. In a classified report there may be a summary of critical information, without a description of sources and methods that is below a designated line on the report. This portion is "torn off" of the report making it Sensitive But Unclassified (SBU) and may be disseminated to law enforcement personnel who do not have a security clearance as "Law Enforcement Sensitive. "

Source: David L. Carter. Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies. Dept. of Justice, Office of Community Oriented Policing Services, 2004. 85 n.118, http://www.cops.usdoj.gov/default.asp?Item=1404

2. A "tear line" is the place on an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the "need to know" principle and foreign disclosure guidelines, of the information below the tear line.

Source: Director of Central Intelligence "Directive 1/7 Security Controls on the Dissemination of Intelligence Information." 3.6. June 30, 1998, http://www.fas.org/irp/offdocs/D.C.id1-7.html

**Technical Data**

Information governed by reference (w) and the Export Administration Regulation (EAR) (reference (z)) The export of technical data that is inherently military in character is

controlled by reference (w). The export of technical data that has both military and civilian uses is controlled by reference (z).

Source: DoD. National Industrial Security Manual (NISPOM). DoD 5220.22-M, February 28, 2006, https://www.dss.mil/GW/ShowBinary/DSS/isp/fac_clear/download_nispom.html

**Technical Information**
Information including scientific, which relates to research, development, engineering, test, evaluation, production, operation, use and maintenance of munitions, and other military supplies and equipment.

Source: Defense Acquisition University. *Glossary: Defense Acquisition Acronyms and Terms.* 11th ed., 2003, http://www.dau.mil/pubs/Glossary/preface.asp

**Technical Reports Automated Information Lists (TRAIL)**
A group of 25 subject-based electronic mail lists designed to make users aware of DTIC's most recently added unclassified/unlimited reports.

Source: Defense Technical Information Center (DTIC). Public STINET Glossary. http://stinet.dtic.mil/help/acronyms.html

**Technical Surveillance Countermeasures (TSCM)**
1. Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected.

Source: Department of Defense. DoD of Military and Associated Terms. JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

2. Techniques and measures to detect, neutralize, and/or exploit a wide variety of hostile and foreign penetration technologies that are used to obtain unauthorized access to classified and sensitive information.

Source: DoD Directive 5240.5, "Technical Surveillance Countermeasures (TSCM) Program. February 22, 2006, http://www.dtic.mil/whs/directives/corres/html/524005.htm

**TEMPEST (Transient Electromagnetic Pulse Surveillance Technology)**
1. Refers to investigations and studies "of compromising emanations associated with information processing systems, as related to classified information."

Source: Ellis Mount. *Top Secret/Trade Secret*. Neal-Schuman, 1985.

2. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when they are transmitted, received, handled, or otherwise processed by any information processing equipment. Because the details of many TEMPEST issues are classified and controlled under strict conditions of need-to-know, unclassified discussions must be somewhat general.

Source: FAS Project on Intelligence Reform, http://www.fas.org/irp/program/security/tempest.htm and http://www.fas.org/sgp/library/nispom/chap_11.htm

**Terrorism Information**

***See Information Sharing Environment***

The term `terrorism information' means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to-- (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
(C) communications of or by such groups or individuals; or
(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Source: Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458, 118 Stat. 3638, http://thomas.loc.gov/cgi-bin/query/D?c108:4:./temp/~c108LGI8Vk::

**Also see:** Elizabeth Martin, "Terrorism and Related Terms in Statute and Regulation: Selected Language" *CRS Report to Congress* December 5, 2006. http://fpc.state.gov/78437.htm (note the link to .pdf is to FAS - Does State encounter the same difficulty in obtaining CRS reports?).

**Terrorism Information Awareness**

***See Data Mining, Total Information Awareness***

Previously known as Total Information Awareness, this name created in some minds the impression that TIA was a system to be used for developing dossiers on U. S. citizens. That is not DoD's intent in pursuing this program. Rather, DoD's purpose in pursuing these efforts is to protect U. S. citizens by detecting and defeating foreign terrorist threats before an attack. To make this objective absolutely clear, DARPA has changed the program name to Terrorism Information Awareness.

Terrorism Information Awareness (TIA) is a research and development program that will integrate advanced collaborative and decision support tools; language translation; and data search, pattern recognition, and privacy protection technologies into an experimental prototype network focused on combating terrorism through better analysis and decision making. If successful, and if deployed, this program of programs would provide decision-and policy-makers with advance actionable information and knowledge about terrorist planning and preparation activities that would aid in making informed decisions to prevent future international terrorist attacks against the United States at home or abroad. In short, DoD's aim in TIA is to seek to make a significant leap in technology to help those working to "connect the dots" of terrorist-related activity. A TIA-like system/ network could provide the defense and intelligence communities with tools and methods to solve many of the problems that have been identified in the aftermath of the attacks against the United States on September 11, 2001, 2 and that are related to improving information analysis in our continuing war against terrorism.

Source: DARPA. "Executive Summary." *Report to Congress regarding the Terrorism Information Awareness Program,* http://www.eff.org/Privacy/TIA/TIA-report.html

**Terrorism Information Prevention System (Operation TIPS)**

1. The program was announced in concept in January 2002 for the stated purpose of creating a national information sharing system for specific industry groups to report suspicious, publicly observable activity that could be related to terrorism. The program is scheduled to be operational in the fall of 2002 as one of the new Citizen Corps programs.

The initiative's design is based on existing programs, such as Highway Watch and Coast Watch, that allow truckers and ship captains to report dangerous conditions along their routes. In response to significant demand among industry groups, Operation TIPS would make these programs available nationwide by providing specific industry groups a single phone number for reporting potentially terrorist-related activities occurring in public areas. Specifically, industry groups have looked to the Justice Department to offer a reliable and cost-effective system that their workers could use to report information to state, local, and federal law enforcement agencies about unusual activities they might observe in the normal course of their daily routines.

Source: TIPS "Citizen Corps" Webpages cached @ The MemoryHole http://www.thememoryhole.org/policestate/tips-deleted.htm ; also see Jay Stanley and Barry Steinhardt. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society." ACLU, January 2003, http://www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39

2. Any and all activities of the Federal Government to implement the proposed component program of the Citizen Corps known as Operation TIPS (Terrorism Information and Prevention System) are hereby prohibited.

Source: Homeland Security Act of 2002. Section 880, http://www.fas.org/sgp/congress/2002/hr5710-111302.html

3. Trained by the FBI, "Hundreds of police, firefighters, paramedics and even utility workers have been trained and recently dispatched as "Terrorism Liaison Officers" in Colorado and a handful of other states to hunt for "suspicious activity" — and are reporting their findings into secret government databases." (Finley)

See attorney Mark Silverstein's observation that recruitment of "Terrorism Liaison Officers" (TLOs) is reminiscent of TIPS. (Rothschild)

Source: Bruce Finley "Terror watch uses local eyes 181," *Denver Post* June 28, 2008, http://www.denverpost.com/news/ci_9725077 and Matthew Rothschild, "Bush's Secret Army of Snoops and Snitches" *The Progressive* July 9, 2008, http://www.alternet.org/rights/90829/

**Terrorist Finance Tracking Program**

***See Society for Worldwide Interbank Financial Telecommunication (SWIFT)***

1. The Terrorist Finance Tracking Program, whose existence was kept secret…is run by the Central Intelligence Agency and overseen by the U.S. Treasury Department. Through it, counterterrorism analysts request information on activities by suspected terrorists from the databases of the Society for Worldwide Interbank Financial Telecommunication, or SWIFT, a Belgium-based, bank-owned entity that collects and relays financial message traffic between thousands of banks in more than 200 countries.

Source: Liz Moyer. Swift Defense. *Forbes* June 23, 2006, http://www.forbes.com/2006/06/23/swift-terrorist-money-transfer-cx_lm_0623swift.html

2. Whereas following the September 11, 2001 terrorist attacks, the President, with the support of Congress, directed the Federal Government to use all appropriate measures to identify, track, and pursue not only those persons who commit terrorist acts here and abroad, but also those who provide financial or other support for terrorist activity;

Whereas consistent with this directive, the United States Government initiated a lawfully classified Terrorist Finance Tracking Program and the Secretary of the Treasury issued lawful subpoenas to gather information on suspected international terrorists through bank transaction information;

Whereas under the Terrorist Finance Tracking Program, the United States Government only reviews information as part of specific terrorism investigations and based on intelligence that leads to targeted searches, such as searches of a specific individual or entity;

Whereas the Terrorist Finance Tracking Program is firmly rooted in sound legal authority based on Executive Orders and statutory mandates, including the International Emergency Economic Powers Act of 1977 and the United Nations Participation Act;

Whereas the Terrorist Finance Tracking Program consists of the appropriate and limited use of transaction information while maintaining respect for individual privacy; [continued].

Source: "Whereas the United States is currently engaged in a global war on terrorism to prevent future attacks against American civilian and military interests at home and abroad" H. Res 895 109th Congress, 2d Session June 28, 2006. Thomas, http://thomas.loc.gov/cgi-bin/query/D?c109:1:./temp/~c109PPeoPw:

3. Treasury cites Executive Order 13224, 3 "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism," as authority for the SWIFT program as a component of its "Terrorist Financing Tracking Program." E.O. 13224 was issued by President Bush on September 23, 2001, pursuant to the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-1706. IEEPA permits the President to exercise broad powers over property or financial transactions, including transfers of credit or payments through banking institutions and securities or other obligations, that involve any interest of a foreign country or a national of that country. To invoke its authorities, the President must declare a national emergency based on the existence of an unusual or extraordinary threat to U.S. national security, foreign policy, or economy having its source, in whole or substantial part, outside the United States.

Finding that foreign terrorist acts, including those of September 11, and threats of future terrorism constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, President Bush issued E.O. 13224. It delegates to the Secretary of the Treasury all necessary authority under IEEPA to block

the assets within U.S. jurisdiction of named individuals and entities who are determined by the Secretary of State and the Secretary of the Treasury, in consultation with each other and with the Attorney General, to pose a significant risk of terrorism or to be assisting, sponsoring, or providing financial, material, or technological support for terrorist acts or designated persons.

Source: Jennifer K. Elsea and M. Maureen Murphy. "Treasury's Terrorist Finance Program's Access to Information Held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)." *CRS Report to Congress* July 6, 2006, http://www.fas.org/sgp/crs/natsec/RS22469.pdf

**Terrorist Identities Datamart Environment (TIDE)**
Hosted by the NCTC and distributed by the Terrorist Screening Center (TSC), that provides consolidated and validated information on terrorist identities to a wide range of customers...

Source: ISE, *Annual Report to Congress on the Information Sharing Environment* 2008, http://www.fas.org/irp/agency/ise/2008report.pdf

**Terrorist Screening Center**
***See TIPOFF, Watch Lists***

1. Attorney General John Ashcroft, Secretary of Homeland Security Tom Ridge, Secretary of State Colin Powell, FBI Director Robert Mueller, and Director of Central Intelligence George Tenet announced the creation of the Terrorist Screening Center (TSC) to consolidate terrorist watchlists and provide 24/7 operational support for thousands of Federal screeners across the country and around the world.

Consolidating Information: The TSC will receive the vast majority of its information about known or suspected terrorists from the TTIC after TTIC has assembled and analyzed that information from a wide range of sources. In addition, the FBI will provide the TSC with information about purely domestic terrorism, i.e., having no connection to international terrorist activities. The TSC will consolidate this information into an unclassified terrorist screening database and make the database accessible to queries for federal, state, and local agencies for a variety of screening purposes.

The TSC, through the participation of the Department of Homeland Security, Department of Justice, Department of State, and Intelligence Community representatives, will determine which information in the Database will be available for which types of screening.

Safeguarding Information: The TSC will not independently collect any information on U.S. citizens. In fact, the TSC does not collect information at all – it only receives information provided by the TTIC and the FBI. The TTIC will provide to the TSC all appropriate and necessary information connected to international terrorism about any individuals – U.S. citizens or not – that TTIC partner agencies hold pursuant to their own authorities, and the FBI will provide to the TSC appropriate and necessary information concerning domestic terrorism, regardless of whether it involves U.S. citizens. If the TSC receives information on U.S. citizens connected with terrorism, its use of that information is subject to the same legal limitations to which it would be subject if the information were not included in the Database.

Source: Department of Justice. “Terrorist Screening Center Fact Sheet.” 2003, http://www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm

2. The Department of State is proud to be part of the Terrorist Screening Center," Secretary of State Powell said. "This cooperative effort will help the United States fight terrorism by identifying visa applicants and others who are known to be threats to our security, before they can do us harm. Combining the knowledge of the FBI, Department of Justice, Intelligence Community, Department of Homeland Security and the Department of State's TIPOFF program is a long-desired goal that is now reality. We are gratified that the State Department's TIPOFF program, which contains over 100,000 names of potential terrorists, will form the basis for both the TTIC and TSC databases. Real-time access by our consular officers to the information provided by the other agencies will make visa issuance more secure and better protect America's borders. We look forward to a successful partnership with our fellow agencies in the war on terrorism.

Source: White House press release. “New Terrorist Screening Center Established.” September 16, 2001, [See the Wayback Machine, http://web.archive.org/web/20080307005324/http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html ]

3. A multi-agency organization administered by the Federal Bureau of Investigation (FBI) that consolidates terrorist watchlist information and provides 24-hour, 7-day a week operational support for federal, state, local, and foreign governments.1 The TSC was created by the September 16, 2003, Homeland Security Presidential Directive-6 (HSPD-6), which directed the TSC to integrate all existing U.S. government terrorist watchlists and assist in the screening of individuals who, for example, apply for a visa, attempt to enter the United States through a port-of-entry, attempt to travel internationally on a commercial airline, or are stopped by a local law enforcement officer for a traffic violation. Prior to the establishment of the TSC, the federal government relied on at least a dozen separate terrorist watchlists maintained by different federal agencies.

Specifically, we identified 20 watchlist records on suspected or known terrorists that were not made available to the frontline screening agents (such as a border patrol officer, visa application reviewer, or local police officer) for use during watchlist screening encounters (such as at a border crossing, through the visa application process, or during a routine traffic stop). We also found that the number of duplicate records in the database has significantly increased since our last review. (p.ii).

Source: DOJ, Office of the Inspector General, Follow-Up Audit of the Terrorist Screening Center, Audit Report 07-41, September 2007,

http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf and ISE, *Annual Report to Congress on the Information Sharing Environment* 2008, http://www.fas.org/irp/agency/ise/2008report.pdf

**Terrorist Surveillance Program (TSP)**

Warrantless surveillance conducted by the National Security Agency and suspended late 2006-early 2007 in favor of the FISA Court.

Source: OMB Watch, "NSA Warrantless Spying Program Shut Down, but Questions Remain," June 23, 2007 http://www.ombwatch.org/article/articleview/3690/ and the 2006 case *ACLU vs. NSA,* http://www.aclu.org/safefree/nsaspying/index.html. Audio at: http://w2.eff.org/legal/cases/att/ACLUappealargument.mp3

**Terrorist Watchlist Person Data Exchange Standard**

**See Global Justice XML Data Model, *Terrorist Threat Integration Center***

From the memorandum of understanding between the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence:

> Provide a data exchange format for terrorist watchlist data that supports the Department of State, Department of Justice, Intelligence Community under the Director of Central Intelligence, and the Department of Homeland Security to develop and maintain, to the extent permissible by law, the most thorough, accurate, and current information possible about individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism

In June 2003, the IC MWG chartered a panel comprised of representatives from the FBI, the Department of State, the National Intelligence Agencies, the IC MWG, the Terrorist Threat Integration Center, the Department of Defense, and the Department of Homeland Security to establish a terrorist watchlist person data exchange standard (TWPDES). The panel drew on a variety of reference information, including selecting standards and agency implementations, to produce a watchlist exchange data structure as a W3C XML schema, backed up by a class model, a data element dictionary, and supporting documentation.

The primary references used by the panel were the person-of-interest class from an NSA entity-of-interest class model, and two Department of Justice sources: The Justice XML Data Dictionary (prerelease 3.0.0) and the National Crime Information Center codes.

The panel was augmented at times by representatives of MITRE Corporation, who specialize in the components of proper names, and by representatives of the DoD Biometrics Management Office, which is promulgating the Common Biometric Exchange File Format.

Source: Intelligence Community Metadata Working Group. http://icmwg.org/person/introduction.asp [Page removed, not at Wayback Machine]

### ThinThread

The National Security Agency pilot program developed in the late 1990s that would have enabled it [NSA] to gather and analyze huge amounts of communications data without running afoul of privacy laws. But after the Sept. 11 attacks, it shelved the project - not because it failed to work but because of bureaucratic infighting and a sudden White House expansion of the agency's surveillance powers, according to several intelligence officials. ThinThread was developed to handle greater volumes of information, partly in expectation of threats surrounding the millennium celebrations. Sources say it bundled four cutting-edge surveillance tools. The agency opted instead to adopt only one component of the program, which produced a far less capable and rigorous program. It remains the backbone of the NSA's warrantless surveillance efforts, tracking domestic and overseas communications from a vast databank of information, and monitoring selected calls.

Source: Siobhan Gorman. "NSA rejected system that sifted phone data legally." *Baltimore Sun* May 18, 2006 [No longer online. Check at your local library].

### Third-Agency Rule

1. The governing rule that states that except as provided in section 102, National Security Act of 1947, classified information originating in one U.S. agency (e.g. DoD) will not be disseminated by another agency to which the information has been made available without the consent of the originating agency.

Source: DoD. Army Regulation AR381-45. "Investigative Records Repository." August 25, 1989. http://www.army.mil/usapa/epubs/pdf/r381_45.pdf, and National Security Act of 1947. http://www.intelligence.gov/0-natsecact_1947.shtml#s102

2. When considering disseminating sensitive material, a law enforcement organization should impose the "Third Agency Rule." This means that any recipient of intelligence is prohibited from sharing the information with another (i.e., third) agency. This affords some degree of control and accountability, yet may be waived by the originating agency when appropriate.

Source: DOJ, *Law Enforcement Intelligence Classifications*, *Products and Dissemination*, November 23, 2004, http://www.cops.usdoj.gov/pdf/e09042536_Chapter_06.pdf

### Threat

In the security technology context, the likelihood that attempts will be made to gain unauthorized access to information or facilities.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/

**Threat Analysis**
Examination of information to identify the elements comprising a threat.

Source: Committee for National Security Systems (CNSS). Instruction 4009. National Information Assurance Glossary, June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

**TIARA (Tactical Intelligence and Related Activities)**
Tactical Intelligence and Related Activities comprised of the array of reconnaissance and target acquisition programs that are a functional part of the basic military force structure and provide direct information support to military operations.

Source: Permanent Select Committee on Intelligence. House of Representatives, One Hundred Fourth Congress. *IC21: The Intelligence Community in the 21st Century,* http://www.access.gpo.gov/congress/house/intel/ic21/ic21_toc.html and Richard A. Best, Jr. "Intelligence, Surveillance, and Reconnaissance (ISR) Programs: Issues for Congress." *CRS Report to Congress February* 22, 2005, http://www.fas.org/sgp/crs/intel/RL32508.pdf

**TIPOFF**
***See Terrorist Screening Center***
The U.S. government's principal terrorist watch list database prior to HSPD-6. TIPOFF is a classified computer lookout system, which was maintained by the DOS's [Department of State, Bureau of Intelligence Research] INR to identify and watch-list known and suspected terrorists. Created in 1987, it originally consisted of 3x5 index cards in a shoe box.

Beginning in 1987, the DOS [Department of State] began keeping watch list (lookout) records on known and suspected terrorists through a system known as TIPOFF. While the DOS had maintained computerized visa records since 1965, including watch lists, the events surrounding the first World Trade Center bombing in 1993 prompted the CA to accelerate the development of the Consular Lookout and Security System (CLASS), so that, among other records, TIPOFF-generated terrorist watch list records could be more easily and efficiently searched by computer at U.S. consular posts and embassies abroad. Consular, intelligence, immigration, and law enforcement officers nominate individuals for inclusion in TIPOFF.

Source: William J. Krouse. "Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6." *CRS Report to Congress* April 21, 2004.
http://www.fas.org/irp/crs/RL32366.pdf

**TOLLS**

***See Data Mining***

Drug Enforcement Agency. Is a database of telephone calls from court ordered and approved wiretaps and Title III investigations. Information such as telephone numbers, time and date of calls, and call duration is captured. Data are mined for patterns to give leads in investigations of drug trafficking;
Purpose: Detecting criminal activities or patterns;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: No;
Features: Other agency data: No.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Top Secret-Cleared U.S. Citizen**:
A citizen of the United States who **has** undergone a background investigation by an authorized U.S. Government Agency and been issued a Top Secret security clearance in accordance with Executive Orders 12968 and 10450 and implementing guidelines and standards published in 32 CFR Part 147.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://www.state.gov/m/a/dir/regs/

**Top Secret Control Number**
Consists of the control symbol of the organization element, the last two digits of the calendar year, the consecutive number of the Top Secret document originated or received that year, and the copy number. For example:

If the Top Secret control number is LND-89/17, copy 3, LND is the TS control number for London; 89 is the calendar year; 17 indicates the 17th TS document either originated or received at post that year; and copy 3 indicates the third copy made of LND-89/17.

Source: Department of State. *Foreign Affairs Manual*. 12 FAM 530, "Storing and Safeguarding Classified Material." http://www.state.gov/m/a/dir/regs/

**Total Information Awareness**

***See Asymmetric Information, Data Mining, Terrorism Information Awareness***

Defense Advanced Research Projects Agency (DARPA) program headed by Information Awareness Office Director John Poindexter, and is now known as the Terrorism Information Awareness Office. As "the key to fighting terrorism is information," TIA's mission was to develop data-mining, knowledge discovery tools, and predictive [terrorist/terrorism] models, that would "imagine, develop, apply, integrate, demonstrate and transition information technologies, components and prototype, closed-loop, information systems that will counter asymmetric threats by achieving total information awareness useful for preemption; national security warning; and national security decision making."

Source: Electronic Frontier Foundation "Total Information Awareness." http://www.eff.org/Privacy/TIA/, http://www.eff.org/Privacy/TIA/20030523_tia_report_review.php, John Poindexter, "Overview of the Information Awareness Office." (archived at FAS http://www.fas.org/irp/agency/dod/poindexter.html), and DARPA. Information Awareness Office site (archived at The Memory Hole), http://www.thememoryhole.org/policestate/iao-logo.htm

**Tradecraft**

The best practices of the Intelligence Community (IC) are termed tradecraft. In the early 1990s, analytic tradecraft were collected in technical notes and used for training. *A Compendium of Analytic Tradecraft Notes* was published in 1996.

Source: Edward Waltz. *Knowledge Management in the Intelligence Enterprise*. Boston: Artech House, 2003. 151-152; *A Compendium of Analytic Tradecraft Notes,* Volume I (Notes 1-10), http://www.au.af.mil/au/awc/awcgate/cia/tradecraft_notes/contents.htm

**Trademark**

A word, phrase, symbol or design, or combination of words, phrases, symbols or designs, which identifies and distinguishes the source of the goods or services of one party from those of others. A service mark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product.

Source: U.S. Patent and Trademark Office. http://www.uspto.gov/

**Transclassification**

Information removed from the RD category by a joint determination of DOE and DOD and placed in the FRD category in accordance with section 142d of the Atomic Energy Act. This information is primarily related to the military utilization of atomic weapons and can be

adequately safeguarded as NSI. This authority is severely restricted and cannot be exercised by RD Classifiers. Contact the DOE for information.

Source: DoD. Defense Personnel Security Research Center. "Employees Guide to Security Responsibilities," http://www.hq.nasa.gov/office/ospp/securityguide/Home.htm

### Trap and Trace Device

Section 3127(4) of title 18, United States Code, is amended—
(A) by striking "of an instrument" and all that follows through the semicolon and inserting "or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;"; and (B) by inserting "or process" after "a device".

Source: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2000, section 216, http://purl.access.gpo.gov/GPO/LPS17579

### Truthful Messages

According to "documents and interviews with contractors, government officials and military personnel," the U.S. government "has been conducting an information war that is extensive, costly and often hidden." The goal is "to counter anti-American sentiment in the Muslim world." The 1,200-strong Fourth Psychological Operations Group based at Fort Bragg, North Carolina, "turns out what its officers call 'truthful messages' to support" the government's objectives.

Source: Jeff Gerth, "Military's Information War Is Vast and Often Secretive." *New York Times* December 11, 2005. http://www.nytimes.com; Alexander Cockburn "CNN and PSYOPS," March 26, 2000, http://www.counterpunch.org/cnnpsyops.html

### TSP

***See Foreign Intelligence Surveillance Act (FISA), State Secrets Privilege***

A secret program (hereinafter "TSP") undisputedly inaugurated by the National Security Agency (hereinafter "NSA") at least by 2002 and continuing today, which intercepts without benefit of warrant or other judicial approval, prior or subsequent, the international telephone and internet communications of numerous persons and organizations within this country. The TSP has been acknowledged by this Administration to have been authorized by the President's secret order during 2002 and reauthorized at least thirty times since.

The Permanent Injunction of the TSP requested by Plaintiffs is granted inasmuch as each of the factors required to be met to sustain such an injunction have undisputedly been met.59 The irreparable injury necessary to warrant injunctive relief is clear, as the First and Fourth Amendment rights of Plaintiffs are violated by the TSP. See *Dombrowski v. Pfister*, 380 U.S. 479 (1965). The irreparable injury conversely sustained by Defendants under this injunction may be rectified by compliance with our Constitution and/or statutory law, as amended if necessary. Plaintiffs have prevailed, and the public interest is clear, in this matter. It is the upholding of our Constitution. As Justice Warren wrote in *U.S. v. Robel*, 389 U.S. 258 (1967): Implicit in the term 'national defense' is the notion of defending those values and ideas which set this Nation apart. . . . It would indeed be ironic if, in the name of national defense, we would sanction the subversion of . . . those liberties . . . which makes the defense of the Nation worthwhile.

Source: *ACLU v. National Security Agency,* August 17, 2006, http://www.aclu.org/images/nsaspying/asset_upload_file689_26477.pdf

### Twilight Information

***See Categorical Exclusion, National Security, Partition, Redaction, Secrecy***

Twilight Information "lies somewhere between deep concealment and full disclosure" (Thompson).[62] Competing elements of secrecy and partial disclosure are the bipolar elements of twilight information. Twilight information may be partially released through (redacted) Freedom of Information Act requests, consist of information previously considered classified, sensitive, or proprietary, or simply be omitted due to regulatory perceptions of no risk, as in the case of NEPA's categorical exclusion.

Twilight information has its roots in the Reagan Administration National Security Directive NSDD-145, which authorized the National Security Agency (NSA) to develop means to protect "unclassified sensitive information." NSDD-145 permitted NSA to control the dissemination of government, government-derived, and non-government information that might "adversely affect the national security." NSDD-145 has had a powerful impact on librarians, publishers, scientists, and citizens who argue that national security classification already exists to protects sensitive information.

Source: Definition, Maret; United States. National Commission on Libraries and Information Science (NCLIS). *Hearing on Sensitive But Not Classified Information*, Washington, D.C.: 1988, and Herbert N. Foerstel. *Secret Science: Federal Control of American Science and Technology*. Westport, CT: Praeger, 1993, (Especially Chapter 5, "Secret But Not Classified")

[62] Remarks of Senator John Kerry in speaking of Senate colleague Daniel Moynihan: "…our vast intelligence apparatus, built to sustain America in the long twilight struggle of the Cold War continues to grow at an exponential rate." *Congressional Record* May 1, 1997, http://www.fas.org/sgp/congress/kerry.html

## ~ U ~

**U2**

*See Classification Markings / Control Markings*

A classification and distribution statement to describe unclassified, unlimited distribution documents and citations approved for public release.

Source: Defense Technical Information Center (DTIC). "Public STINET Glossary." http://stinet.dtic.mil/help/acronyms.html

**UL**

*See Classification Markings / Control Markings*

A classification and distribution statement to describe unclassified, unlimited distribution documents and citations. These documents must be requested on DTIC Form 55 (Request for Release of Limited Document) if you do not have permission to view or order the document.

Source: Defense Technical Information Center (DTIC). "Public STINET Glossary." http://stinet.dtic.mil/help/acronyms.html

**Unacknowledged SAP**

*See Special Access Programs*

A SAP having protective controls ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information.

Source: DoD Directive 5205.7 "Special Access Program (SAP) Policy." January 5, 2006, http://www.dtic.mil/whs/directives/corres/html/520507.htm

**Unauthorized Disclosure**

1. Communication or physical transfer of classified information to an unauthorized recipient.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information." http://www.archives.gov/federal-register/executive-orders/2003.html , and DoD Directive 5210.50. Unauthorized Disclosure of Classified Information to the Public.

2. The compromise of classified information by communication or physical transfer to an unauthorized recipient. It includes the unauthorized disclosure of classified information in a newspaper, journal, or other publication where such information is traceable to an agency because of a direct quotation or other uniquely identifiable fact.

Source: U.S. Department of State. *Foreign Affairs Manual*. 12FAM090, "Definitions of Diplomatic Security Terms." November 13, 2003, http://foia.state.gov/REGS/Search.asp

**Unclassified But Restricted Information**
***See Restricted***

**Unclassified But Sensitive**
***See Sensitive But Unclassified***

**Unclassified Controlled Nuclear Information (UCNI)**
***See DoD Unclassified Controlled Nuclear Information (DoD UCNI)***

1. A DOE classification to prevent the unauthorized dissemination of unclassified information on physical security for special nuclear material, critical installations, and equipment.

Source: U.S. Department of Energy. "Unclassified Controlled Nuclear Information Topical Guideline for DOE Facility and Site Reviews." http://www.osti.gov/html/osti/opennet/document/tg-fsr-1/tg-fsr-1.html

2. The Atomic Energy Act of 1954, as amended, created Unclassified Controlled Nuclear Information, among other categories of information. Unclassified Controlled Nuclear Information is certain unclassified Government information whose unauthorized dissemination is prohibited. This information concerns atomic energy defense programs; pertains to the design of production facilities or utilization facilities; security measures for the physical protection of production or nuclear material storage facilities; or the design or manufacture of any nuclear weapon or component which was declassified or removed from the Restricted Data category.

…the Secretary of Energy (hereinafter in this section referred to as the "Secretary"), with respect to atomic energy defense programs, shall prescribe such regulations, after notice and opportunity for public comment thereon, or issue such orders as may be necessary to prohibit the unauthorized dissemination of unclassified information pertaining to

(A) the design of production facilities or utilization facilities;

(B) security measures (including security plans, procedures, and equipment) for the physical protection of
(i) production or utilization facilities,
(ii) nuclear material contained in such facilities, or
(iii) nuclear material in transit; or
(C) the design, manufacture, or utilization of any atomic weapon or component if the design, manufacture, or utilization of such weapon or component was contained in any information declassified or removed from the Restricted Data category by the Secretary (or the head of the predecessor agency of the Department of Energy) pursuant to section 2162 of this title.

Source: 42 U.S.C. 2168. http://www.gpoaccess.gov/U.S.C.ode/; Atomic Energy Act, Chapter 12 section 148 and DOE, Safeguards and Security Information Security Handbook. http://www.pnl.gov/isrc/text.stm and Department of Energy. "Unclassified Controlled Nuclear Information, General Guideline GG-5." February 2004, http://www.fas.org/sgp/othergov/doe/ucni.pdf

**Unclassified/For Official Use Only (U/FOUO)**

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized security personnel without further approval from DHS.
(U) This product contains U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight or information handling procedures.

Source: DHS, *Domestic Extremism Lexicon Reference Aid*, March 26, 2009, http://www.scribd.com/doc/14884903/Domestic-Extremism-Lexicon-US-Department-of-Homeland-Security-Reference-Aid

**Unclassified Information**

***See Sensitive But Unclassified Information***

1. Information that has not been determined pursuant to EO 12958 or any predecessor order to require protection against unauthorized disclosure and that is not designated as classified.

Source: Committee for National Security Systems (CNSS). Instruction 4009. *National Information Assurance Glossary*. June, 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

and EO 12958 "Classified National Security Information," Amended, http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2

2. Civic-related information to which, in its original for, the general public had direct access (i.e., public records); and Newspaper, magazine, and periodical clippings dealing with specific criminal categories.

Source: David L. Carter. *Law Enforcement Intelligence: a Guide for State, Local, and Tribal Law Enforcement Agencies.* Dept. of Justice, Office of Community Oriented Policing Services, 2004, http://www.cops.usdoj.gov/default.asp?Item=1404 ; Also see: James J. Bagley. "Understanding Government Controls on Unclassified Information or Who's on First?" NCMS Viewpoints 1 (1993), http://www.fas.org/sgp/eprint/bagley.html

**Unclassified Intelligence**

"Intelligence is information, which has been discovered, discriminated, distilled, and disseminated in a form tailored to the needs of a specific policymaker at a specific time and place."

Source: Robert David Steele. "Virtual Intelligence: Conflict Avoidance and Resolution Through Information Peacekeeping." http://www.usip.org/virtualdiplomacy/publications/papers/virintell.html

**Unclassified Limited**

Information exempt from public release by the Freedom of Information Act or other statutory authority. A DoD directive issued in 1970 established distribution limitations on technical reports which used the term. Unclassified Unlimited applied to information which was approved for public release by competent authority--an individual or organization authorized to release the information to the public, whether foreign or domestic.

Unclassified Limited meant that some official reason supported withholding information in technical reports from public release without approval by appropriate authority. The directive also provided reasons why a report should not be released to the public except upon approval by the contracting agency. The current directive that governs distribution limitation for technical reports is DoD 5230.24, Distribution Statements on Technical Documents. **Examples of Limitations on Unclassified Information**:

- Freedom of Information Act (5 USC 552)
- Unclassified Controlled Nuclear Information (20 CFR 1017.1)
- DoD Unclassified Controlled Nuclear Information (10 USC 128)
- International Traffic in Arms Regulation (22 USC 2778 (a))
- Export Control Administration Regulation (FEB 1992, EAA of 1979) Dual-Use Information

- Unclassified National Security Related Information (DoD 15210.74)
- Sensitive but Unclassified Information (COMSEC/ISM)
- Withholding of Unclassified Technical Data from Public Disclosure (DODD 5230.25, PL 98-94) (10 USC 130)
- Militarily Critical Technologies List
- Distribution Statements on Technical Documents (DODD 5230.24)
- Limited Official Use Information
- Computer Security Act of 1987 (PL 100-235) Sensitive Information
- Drug Enforcement Administration Sensitive Information
- COMSEC Supplement to the DoD ISM Sensitive Information and Technologies

Source: James J. Bagley. "Understanding Controls on Unclassified Government Information or Who's on First?." Reposted with permission from *NCMS Viewpoints* 1, 1993 (a publication of the National Classification Management Society), http://www.fas.org/sgp/eprint/bagley.html

**Undisclosed Information**

29) Chapter Three is added following Article 54 for protection of Undisclosed Information. CPA/ORD/26 April 2004/81 8:

30)Article 1 is added as the first article in Chapter Three to read as follows: "Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

b) has commercial value because it is secret; and

c) has been subject to reasonable steps under the circumstances by the person lawfully in control of the information to keep it secret."

Source: Coalition Provisional Authority, "Order 81, which deals with 'Patent, Industrial Design, Undisclosed Information, Integrated Circuits and Plant Variety,' http://www.trade.gov/static/iraq_memo81.pdf

**United States Civilian Internee Information Center**

The national center of information in the United States for enemy and US civilian internees.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**United States Information Agency**

On October 1, 1999, USIA was integrated into the State Department. The Office of the Undersecretary for Public Diplomacy and Public Affairs was created to oversee the public diplomacy programs that USIA administered. USIA's Office of Research and Media Reaction was merged into State's Bureau of Intelligence and Research. USIA's international broadcasting operations were taken over by the newly created Broadcasting Board of Governors. Although State may provide policy guidance and advice, the Board is independent from State.

Source: *U.S. Public Diplomacy: State Department Expands Efforts but Faces Significant Challenges: Report to the Committee on International Relations, House of Representatives*. Washington, D.C.: U.S. General Accounting Office, 2003. http://www.gao.gov/new.items/d03951.pdf; U.S. Department of State. "Department Organization," http://www.state.gov/r/pa/ei/rls/dos/436.htm, and Nancy Snow. *Propaganda, Inc.: Selling America's Culture to the World.* New York: Seven Stories Press, 1998.

**United States Intelligence Board**

In 1958, the US Communications Intelligence Board (USIB) merged with the Intelligence Advisory Committee to form the US Intelligence Board, an element of the National Security Council. In 1976, the USIB was abolished and replaced with the National Foreign Intelligence Board. For info on its organization, see pp. 280ff of Richelson.

Source: Jeffrey Richelson. *The U.S.Intelligence Community.* Cambridge, MA: Ballinger, 1985.

**Unknown**

1. A code meaning "information not available." 2. An unidentified target. An aircraft or ship that has not been determined to be hostile, friendly, or neutral using identification friend or foe and other techniques, but that must be tracked by air defense or naval engagement systems.

Source: Department of the Army. Marine Corps Combat Development Command. Department of the Navy. *Operational Terms and Graphics*. FM 1-02 (FM 101-5). September 21, 2004, http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm#contents and Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Unofficial Information (*Neofitsialnaya informatsiya)***

Information which comes from well-informed individuals, but which is not openly confirmed by the government, administration or officials.

Source: Vasily Mitrokhin, ed. *KGB Lexicon: The Soviet Intelligence's Officer's Handbook*. London: Frank Cass, 2002.

### Upgrade

A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

Source: DoD. National Industrial Security Manual (NISPOM). DoD 5220.22-M, February 28, 2006, https://www.dss.mil/GW/ShowBinary/DSS/isp/fac_clear/download_nispom.html

### Upgrading

The determination that certain classified information requires, in the interests of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect the higher degree.

Source: National Imagery and Mapping Agency. "NIMA Guide to Marking Classified Documents." October 4, 2001, http://www.fas.org/sgp/othergov/DoD/nimaguide.pdf

### Urban Resolve 2015

Urban Resolve is an experiment sponsored by U.S. Joint Forces Command, Joint Experimentation Directorate, Joint Urban Operations Office, with technical assistance from the Institute for Defense Analyses, Joint Advanced Warfighting Program.

It is a distributed simulation to be carried out at the U.S. Joint Forces Command, Joint Experimentation Directorate, Distributed Continuous Experimentation Environment, at the U.S. Army Topographic Engineering Center at Fort Belvoir, Virginia, and at the Space and Naval Warfare Systems Command facilities in San Diego, California.

Source: United States Joint Forces Command, http://www.jfcom.mil/about/experiments/uresolve.htm; the Joint Forces Command podcast can be subscribed to through iTunes Music Store.

### United States Strike Command (USSTRICOM)

United States Strike Command (USSTRICOM) was established in 1961 to furnish deployable, combat-ready forces as in an emergency situation anywhere within the United States or overseas. A two service command (Army and Air Force), USSTRICOM is headquartered at McDill Air Force Base FLA and is commanded by an Army general. It has two major components, the U.S. Army Forces Strikes Command (ARSTRIKE) and the U.S. Air Force Strike Command (AFSTRIKE), are headquartered in close proximity.

Source: United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. *Army Surveillance of Civilians: A Documentary Analysis*. 92nd Congress, second session. Washington, D.C.: U.S. Government Printing Office, 1972. 86.

---

## ~ V~

**Validation of Information**

Procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

Source: Judicial Administration. 28 CFR 23, http://www.gpoaccess.gov/CFR/index.html

**Vaughn Index**

1. Originated from *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), cert. denied, 415 U.S. 977 (1974), wherein the court rejected an agency's conclusory affidavit stating that requested Freedom of Information Act (FOIA) documents were subject to exemption. A Vaughn Index must: (1) identify each document withheld; (2) state the statutory exemption claimed; and (3) explain how disclosure would damage the interests protected by the claimed exemption."

Source: 'Lectric Law Library's Lexicon "Vaughn Index," http://www.lectlaw.com/def2/u049.htm

2. There is no set form of a Vaughn Index although the Vaughn decision requires agencies to prepare an itemized index, correlating each withheld document (or portion) with a specific FOIA exemption and the relevant part of the agency's nondisclosure justification. A Vaughn Index should indicate, for each document, that any reasonably segregable information has been disclosed.

Source: U.S. Department of Justice. Freedom of Information Act Guide, http://www.usdoj.gov/oip/litigation.htm

3. A sample Vaughn motion form that can be submitted to a U.S. district court is included in Appendix C.

Source: Melanson, Philip H. *Secrecy Wars: National Security, Privacy, and the Public's Right to Know.* Washington, D.C.: Brassey's, 2001.

4. An example of a Vaughan Index reflecting documents the CIA withheld from the ACLU regarding torture is here: http://tinyurl.com/yjohpk2

**Verity K2 Enterprise**

***See Data Mining***

Defense Intelligence Agency, Information Analysis and Infrastructure Protection Directorate. Mines data from the intelligence community and Internet searches to identify foreign terrorists or U.S. citizens connected to foreign terrorism activities;
Purpose: Analyzing intelligence and detecting terrorist activities;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: Yes;
Features: Other agency data: Yes.

Source: General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses*. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html & *Electronic Information Privacy Center (EPIC) vs. Department of Defense,* requesting "expedited processing and release of agency records requested by Plaintiff from the Defense Intelligence Agency, a component of Defendant Department of Defense,http://www.epic.org/open_gov/verityk2/complaint.pdf

**Veterans Affairs Central Incident Response Center**

***See Data Mining***

Department of Veterans Affairs Headquarters. Is used to monitor and manage intrusion detection and firewalls. Scripts are written for forensic analysis to go through data collected from system and network logs;
Purpose: Detecting criminal activities or patterns;
Status: Operational;
Features: Personal information: Yes;
Features: Private sector data: Yes;
Features: Other agency data: No.

Source: General Accounting Office. Data Mining: Federal Efforts Cover a Wide Range of Uses. GAO-04-548, May 4, 2004, http://www.gao.gov/htext/d04548.html

**Video News Release**

***See Prepackaged News***

**Violation**

Any knowing, willful, or negligent action that could reasonably be expected to result in an authorized disclosure of classified information; Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

Source: Executive Order 13292 "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information."
http://www.archives.gov/federal-register/executive-orders/2003.html

**Virtual Case File**

1. The last piece of the puzzle is imminent: a relational database with a web interface called Virtual Case File that will collect ALL investigative information relating to criminal cases and national security investigations for FBI employees to search and analyze.

Source: "IT Infrastructure for 21st Century Crime: CIO Zal Azmi Talks About the FBI's Technology Make Over." April 2, 2004, http://www.fbi.gov/page2/april04/040204cioazmi.htm

2. The User Application Component is replacement of user applications that will enhance our ability to access, organize and analyze information. Specifically, the Trilogy Program will migrate five investigative applications into a "Virtual Case File" (VCF), to provide user-friendly, web browser access to mission critical information. A web-based interface will enable our users to have a graphical interface with investigative information. It will eliminate the cumbersome aspects of our current system, greatly enhance our collaborative environment and go a long way towards eliminating the problems obvious from Hanssen and McVeigh.

Source: Testimony of Sherry Higgins, Project Management Executive for the Office of the Director, FBI Before the Senate Judiciary Subcommittee on Administrative Oversight and the Courts, July 16, 2002, "FBI Infrastructure," http://www.fbi.gov/congress/congress02/higgins071602.htm

3. Five-six years of delay, troubles with contractor SAIC (Science Applications International Corporation), and between $104- $170 million spent, FBI Director Robert Mueller told Congress that the Sentinel system "will pave the road starting with our legacy case management system, for subsequent transformation of all legacy applications to modern technology under our Enterprise Architecture."

Source: James C. McGroddy and Herbert S. Lin (Ed.), *A Review of the FBI's Trilogy Information Technology Modernization Program.* National Academies Press, 2004, http://www.nap.edu/catalog/10991.html and Harry Goldstein. "Who Killed the Virtual Case File? *IEEE Spectrum Online* 42 no. 8 (2005), [See the Wayback Machine, http://web.archive.org/web/20080202103506/http://www.spectrum.ieee.org/sep05/1455 ]

**Virtual Proving Ground**
VPG is a distributed, integrated complex of materiel system performance and reliability simulation capabilities that generates valid materiel system effectiveness information by presenting verified modeled stimuli to systems operating in synthetic environments according to realistic procedures and ground truth information.

Source: U.S. Army Developmental Test Command. "Virtual Proving Ground." http://vpg.dtc.army.mil/ [Now a blocked site]

**Visual Information**
Use of one or more of the various visual media with or without sound. Generally, visual information includes still photography, motion picture photography, video or audio recording, graphic arts, visual aids, models, display, visual presentation services, and the support processes. Also called VI.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Voluntary Furnished Confidential Information**
A submission of a record that--
(i) is made to the Department in the absence of authority of the Department requiring that record to be submitted; and (ii) is not submitted or used to satisfy any legal requirement or obligation or to obtain any grant, permit, benefit (such as agency forbearance, loans, or reduction or modifications of agency penalties or rulings), or other approval from the Government.

Source: S. 622 "Restoration of Freedom of Information Act of 2005." http://thomas.loc.gov/cgi-bin/query/z?c109:S.622.IS

---

**~ W ~**

**War Card Database**
The War Card database presents "the Iraq-related public pronouncements of top Bush administration officials to be tracked on a day-by-day basis against their private assessments and the actual 'ground truth' as it is now known. Throughout the database, passages containing false statements by the top Bush administration officials are highlighted in yellow. The 935 false statements in the database may also be accessed by selecting the "False Statements" option from the "Subject" pull-down menu and may be displayed within selected date ranges using the selection tool below."

Source: Center for Public Integrity, http://projects.publicintegrity.org/WarCard/Search/Default.aspx

**Warden System**

An informal method of communication used to pass information to US citizens during emergencies.

Source: Department of Defense. *DoD of Military and Associated Terms.* JP 1-02. As Amended through 17 October 2008, http://www.dtic.mil/doctrine/jel/doddict/

**Warning Notice-Intelligence Sources or Methods Involved**

***See Classification Markings / Control Markings***

**Warning Notices**

***See Classification Markings / Control Markings***

**Warrantless Surveillance**

***See Foreign Intelligence Surveillance (FISA), National Security, Privacy***

1. This President appears to have forgotten that fact. Not only has he asserted the right to go around the FISA court and the wiretap act, but he has actually done so. Even more disturbing, he does not believe that he is accountable to the Congress, the courts or anyone else. This Committee created the FISA statute and the FISA court, yet the President believes we are not entitled to know what he or the courtare doing. The President also believes that we are not entitled to know what he is doing, or has been doing, outside the confines of the FISA statute. Now we have passed a flawed bill that, in the guise of updating the FISA law, actually gives the President almost unfettered power to spy without court supervision, not just on foreigners, but on Americans.

Source: Rep. John Conyers (p.4), United States. Congress. House. Committee on the Judiciary. Warrantless surveillance and the Foreign Intelligence Surveillance Act: the Role of Checks and Balances in Protecting American's Privacy Rights. Pt. I: hearing before the Committee on the Judiciary, House of Representatives, One Hundred Tenth Congress, first session, September 5, 2007, Washington: U.S. G.P.O. 2008, http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=110_house_hearings&docid=f:37599.pdf

2. The government has asserted three interests in engaging in wiretaps for "national security" purposes (apart from wiretapping to detect possible violations of the criminal law, including the laws against espionage, sedition, and treason). These are: (1) gathering foreign intelligence information; (2) preventing information about the United States from reaching foreign intelligence services; and (3) protecting the United States against internal threats to its stability (1975-1976: 133).

In speaking of his own warrantless surveillance, Dr. Halperin (1975-1976: 159-160) writes

> In pre- Watergate days it seemed inconceivable that word of the surveillance would ever leak out. The mistake was in giving such broad power and discretion to executive branch officials. This is why the founding fathers insisted that warrants from a magistrate be required before there could be a search and seizure. Where the "thing" to be seized is information, the need for a warrant is even more urgent.

Source: Morton Halperin, "National Security and Civil Liberties," *Foreign Policy* 21 (Winter, 1975-1976): 125-160.

**Watch Lists**

***See Terrorist Screening Center***

Terrorist and criminal watch list systems--sometimes referred to as watchout, lookout, target, or tip-off systems--are important tools in controlling and protecting our nation's borders. The events of September 11, 2001, and other incidents since then, have highlighted the need to share these watch lists. In light of the importance of border security, GAO was asked to identify federal databases and systems that contain watch lists, the agencies that maintain and use them in protecting our nation's borders, the kind of data they contain, whether federal agencies are sharing information from these lists with each other and with state and local governments and private organizations, the structural characteristics of those lists that are automated, and whether opportunities exist to consolidate these watch lists.

Specifically, nine federal agencies--which prior to the creation of the Department of Homeland Security (DHS) spanned the Departments of Defense, Justice, State, Transportation, and the Treasury--develop and maintain 12 watch lists.

Source: U.S. General Accounting Office. "Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing." GAO-03-322 April 15, 2003, http://www.gao.gov/htext/d03322.html; also see DOJ, OIG, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, Audit Report 09-25, May 2009, http://www.usdoj.gov/oig/reports/FBI/a0925/final.pdf

**Wisdom Warfare**

A cognitive process that has three main components: knowledge, which includes systems that collect raw data, organize it into useful information, analyze it to create intelligence, and assimilate it to gain knowledge; wisdom contains those systems that allow humans to interact with the knowledge to exercise wisdom, which includes modeling and simulation tools; Human

System Integration, or HIS, contains all of the systems necessary to assist decision makers in getting the information needed in the form desired. Once the decision makers understand the information, they can apply experience to make the best decisions.

Source: Lt Col Edward F. Murphy, et al. Information Operations: Wisdom Warfare For 2025, Air Force 2025 volume 1. April, 1996,
http://www.fas.org/spp/military/docops/usaf/2025/v1c1/v1c1-1.htm#CONTENTS

**Working Files**

1. Documents such as rough notes, calculations, or drafts assembled or created and used to prepare or analyze other documents. Also called working papers.

Source: DOE. Chief Information Officer. "Records Management Definitions,"
http://cio.energy.gov/rmdefinitions.pdf

**Working Papers**

Working papers are classified materials (notes, drafts, drawings, etc.) that are generated in the preparation of a finished document. They must be dated when first created. They must also be marked with the overall classification, any applicable speciacial category notice, and the annotation "WORKING PAPERS" on each page and the cover (if any). It is recommended that portion markings be applied at the time of generation to aid in applying proper markings to the finished product.

Source: National Classification Management Society. *Bulletin*. January-February 2005. 4.
https://www.classmgmt.com/Home/ [issue no longer online]

2. Documents or materials, regardless of the media, which are expected to be revised prior to the preparation of finished product for discrimination or retention.

Source. ISOO. *Marking Classified National Security Information*. ISOO Implementing Security Directive 1, September 22, 2003,
http://www.archives.gov/isoo/training/marking-booklet.pdf

**Write-to-Release**

A general approach whereby intelligence reports are written in such a way that sources and methods are disguised so that the report can be distributed to customers or intelligence partners at lower security levels. In essence, write-to-release is proactive sanitization that makes intelligence more readily available to a more diverse set of customers. The term encompasses a number of specific implementation approaches, including sanitized leads and Tearline reporting.

Source: Director of Central Intelligence Directive 8/1. "Intelligence Community Policy on Intelligence Sharing." June 4, 2004, http://www.fas.org/irp/offdocs/D.C.id8-1.html

---

## ~ X, Y, Z ~

**XGDS (Exempt from General Declassification Schedules)**
GDS…begins with the date of issuance, or the date of previously assigned classification.
XGDS-3…is automatically declassified 20 years after date classification is assigned.
XGDS-2…is to be reviewed for declassification 30 years after date classification is assigned.

Source: Departments of the Air Force, The Army, The Navy and Transportation. "IFF MARK X (SIF)/MARK XII Systems Security Classification." January 3, 1975,
[See the Wayback Machine,
http://web.archive.org/web/20050209174612/http://neds.daps.dla.mil/Directives/5510_141.pdf ]

**Xn**
***See Declassification***
Signifies a declassification within 10 years because disclosure could reasonably be expected to cause damage to the national security beyond the 10-year limit; where "n" is the exemption category number as listed in section 1.6 of EO 12958,

Source: Los Alamos National Lab. "Definitions."
http://www.hr.lanl.gov/SCourses/All/PortionMarking/define.htm

**Yankee White**
**See *Nickname***
A rigorous, special security investigation and background check for (military) personnel working with the President. The 89 SPS (U.S. Air Force Security Police Squadron) administers the Yankee White clearance program.

Source: DoD. DoDI 5210.87 "Selection of DoD Personnel and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs)," 11/30/1998.
http://www.dtic.mil/whs/directives/corres/rtf/521055x.rtf and Global Security.org
http://www.globalsecurity.org/wmd/systems/nuclear-football.htm