ALLIED
ENGINEERING
DOCUMENTATION
PUBLICATION

AEDP-2
VOLUME 2
(Edition 1)

NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA)

VOLUME 2: NIIA Management Guidance

AEDP-2
(Edition 1)

SEPTEMBER 2005

NORTH ATLANTIC TREATY ORGANIZATION

NATO STANDARDIZATION AGENCY (NSA)

NATO LETTER OF PROMULGATION

September 2005

1. AEDP-2 (Edition 1) VOLUME 2 - NATO INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR) INTEROPERABILITY ARCHITECTURE (NIIA) VOLUME 2: NIIA MANAGEMENT GUIDANCE - is a NATO UNCLASSIFIED publication.

2. AEDP-2 (Edition 1) is effective upon receipt.

J MAJ
Brigadier General, POL(A)
Director, NSA

FOREWARD

The NATO ISR Interoperability Architecture (NIIA) provides the basis for the technical aspects of an architecture that provides interoperability between NATO nations' ISR systems. It is recognized that a complete architecture requires a technical view, a systems view, and an operational view to be complete. However, the systems and operational views are dependant on the specific scenario, with the systems involved determined by the participating nations, and the operational view defining how the various systems are actually interconnected. While a acquisition group such as Air Group IV could theorize hypothetical scenarios and generate the systems and operational views based on those hypothetical scenarios, it is more important to focus on the technical issues of providing the interconnectivity options within national and NATO-owned systems, and leave the operations planning to the military community.

This AEDP provides the technical and management guidance for implementing the NIIA in ISR systems. It is divided into four volumes. Volume 1 provides the introduction and explanation of the technical architecture. Volume 2 contains guidance for managing the NIIA, specifically, the configuration management and test and certification guidance to the NIIA Custodians. Volume 3 is the technical guidance relevant to multiple parts of the architecture. Finally, Volume 4 provides terms and definitions. The four volumes are published as separate documents due to the large size of each volume.

This volume focuses on providing management guidance to the Custodians tasked with the responsibility for each document. In accordance with NATO policies, a specific Custodian is named for each document. This document provides both configuration management and test and certification policies and guidance to the Custodians.

In addition to AEDP-2, users of the NIIA should obtain copies of each of the STANAGs incorporated into the architecture. These STANAGs provide the key interface standards needed to provide the systems interoperability. Many of the STANAGs also have separate Implementation Guides for the standard, published as separate AEDPs. In addition, specific guidance on sanitization and declassification of advanced memory recording systems (solid state and advanced disk arrays) is provided in a separate document for ease of dissemination. This document is AEDP-3. A complete list of the documents included in the set of STANAGs/AEDPs is in Annex A of Volume 1 of this document.

Questions or comments on this document can be provided to either the Secretary of Air Group IV or the Custodian. Correspondence to the Secretary should be addressed to: Secretary, Air Group IV; Air Armaments Section, International Staff; HQ NATO; B-1110, Brussels, Belgium (telephone: +32-2-707-4291; telefax: +32-2-707-4103). Correspondence to the Custodian should be addressed to: Custodian, AEDP-2; SAF/AQIJ; 1060 Air Force Pentagon; Washington D.C. 20330-1060; United States (telephone +1 703-588-2669; telefax: +1 703-588-1340).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. The NATO ISR Interoperability Architecture (NIIA) defines the overall structure of the elements of the Intelligence, Surveillance, and Reconnaissance (ISR) community. The intent of this document is to provide the context for the standards developed by NATO Air Group IV, as well as commercial and international standards that are applicable to the ISR mission. It should be noted that while the original NIIA document was a description of an imagery-only architecture, the work of Air Group IV has suggested that the scope of the Group's activities should include other sources of intelligence.

2. A description of operational environment, including a number of variations on the basic data flow, is provided. This description includes notional task flow descriptions and timelines. When examining the ISR data flow, it is noted what interfaces will be exercised during the two primary ISR Integration Working Group (ISRIWG) demonstrations. These two demonstrations, one to show interoperability at the input to the ground/exploitation system by using the NATO Advanced Data Storage Interface, and one to show interoperability at the output of the ground/exploitation system by using the NATO Secondary Imagery Format and NATO Standard Imagery Library Interface.

3. Each of the currently ratified and developmental standards developed under Air Group IV is also reviewed. Each standard is discussed in terms of its application and use. Other documents needed to complete the architecture are also discussed.

4. Finally, the actual architecture is introduced and discussed. Four levels of interoperability, as defined in NATO interoperability publications, are reviewed. They are:

- Degree 1: Unstructured Data Exchange. Involves the exchange of human-interpretable unstructured data such as the free text found in operational estimates, analysis and papers.
- Degree 2: Structured Data Exchange. Involves the exchange of human-interpretable structured data intended for manual and/or automated handling, but requires manual compilation, receipt and/or message dispatch.
- Degree 3: Seamless Sharing of Data. Involves the automated sharing of data amongst systems based on a common exchange model.
- Degree 4: Seamless Sharing of Information. An extension of degree 3 to the universal interpretation of information through data processing based on co-operating applications.

5. It should be noted that the objective of the NIIA is to achieve interoperability at Degree 2, with some specific interfaces achieving Degree 3. Degree 4 can be considered a long term objective, but it was determined that lower degrees of interoperability should not be delayed in favour of ultimately achieving a higher degree. Degree 2 interoperability is a significant accomplishment, and will provide a high level of capability to NATO and coalition forces. Higher degrees of interoperability will be addressed once degree 2 is achieved and demonstrated.

6. Finally, a review of the standards as they fit into the architecture is performed. The standards are mapped against the International Standards Organisation (ISO) 7-Layer Interface Model. This mapping is performed to identify how the standards fit together and include commercial and international standards, as well as to identify the holes in the architecture that must be addressed by the activities of the ISRIWG and its subordinate groups. During the analysis, it was determined that most interfaces are adequately defined, and those requiring additional standardization can be filled with existing commercial and/or international standards. The key issue remaining is the multitude of choices provided by many of the standards, thereby allowing multiple implementations that would not

be interoperable. It will be important to develop interface profiles that define the specific choices within each standard, thereby ensuring interoperability.

7. In summary, it is noted that the ISR architecture is applicable across all levels of NATO and coalition operations, including both Article 5 (war operations) and non-Article 5 (peacekeeping, peacemaking, etc.) campaigns. Finally, while it is recognised that the standards are complete, there is a large volume of support documentation, including configuration management plans, test and certification plans, implementation guidance, and acquisition guidance, that are available to the community. It is recommended that STANAG custodians consolidate this documentation into a single volume to accompany each standard. The accepted form of this volume is as an Allied Engineering Documentation Publication (AEDP). Combining the AEDPs with this document and the standards forms the complete NIIA definition and documentation set.

1.0 INTRODUCTION

1.0.1 In the development of the NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA), Air Group IV recognized a need to provide guidance to the Custodians of the numerous Standardisation Agreements (STANAGs) and Allied Publications (APs) on how to manage their respective documents. It is also recognized that flexibility is required in this process, allowing each Custodian to tailor the processes to the needs of the particular document. For example, the size of the user community is different for different standards, and as such, the configuration management processes should be different. Similarly, test and certification of different standards requires different approaches.

1.0.2 This volume of the NIIA document provides the specific instructions to the Custodians on Configuration Management (CM) and Test and Certification activities. It is intended to be taken in the context of the entire AEDP-2 document, including the other portions, as well as the STANAGs and APs that are included in the NIIA. For the complete list of documents, see Volume I, Annex A.

1.1 Scope

This document provides specific policy guidance to the document Custodians on how to manage the configuration as well as the test and certification requirements for each standard included in the NIIA. Configuration management is generally controlled directly by the Custodian with technical support from an editorial team and decision support of some form of configuration control board. Test and certification activities are generally delegated to specialized test facilities that coordinate their activities with the respective Custodians.

2.0 VOLUME CONTENTS

This volume includes two documents that define the top level policy for the Custodians. Annex A defines the configuration management policy, while Annex B discusses that test and certification activities. I t should be noted that in both cases, additional documentation is required from the Custodian. This additional documentation is published generally in the associated Allied Engineering Documentation Publication (AEDP), although the Custodian may be choose to publish the material in other forms. As the specific documents are published, each will be added to the document reference in Volume 1, Annex A.

2.1 Configuration Management Guidance

Annex A provides the top level policy guidance for establishing a configuration control program. This document defines the basic requirements for configuration management, and suggests some options on how to implement the program, as well as criteria for selecting between the options. It should be noted that the guidance requires each Custodian to produce a specific configuration management plan and publish it for the NIIA community. In most cases, it is expected that the configuration management plan be published in an Annex of the respective AEDP, although in some cases, the plan may be published in a different manner.

2.2 Test and Certification Guidance

Annex B provides the top level guidance for the establishment of a test and certification program for the standards. Test and certification is becoming more important as the standards become more complex. Previously, film sizes and placement of titling characters on film were simple enough that they did not require specific testing to verify compliance with the standard. However, with the standards defined in the NIIA, the technical issues are complex enough to require specific tests and demonstrations to verify compliance. With this requirement, it is also appropriate to establish Registries of those products/systems that successfully complete the certification testing so that members of the ISR community in NATO can have a ready source of accurate information on product or system performance. If entirely to industry, historical experience has shown that claims will eventually spread to the point that a statement of compliance is meaningless. By managing the compliance test program within the authority of the Custodian, statements of compliance retain their credibility. As with the configuration management guidance, each Custodian will establish separate test and certification plans and it is expected that these plans will be published in an Annex of the respective AEDP, although in some cases, the plans may be published in a different manner.

3.0 SUMMARY

This document provides management guidance to the Custodians and is intended to be supplemented by additional documentation published by the Custodian. If additional management topics are required, they will be published in future versions of this document through the addition of further Annexes.

FOREWORD

This plan describes the North Atlantic Treaty Organization (NATO) Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA) Configuration Management Policies. The NIIA defines the architecture for exchanging digital ISR data between NATO nations. The NIIA consists of a suite of standards that are assembled under NATO Air Group IV (AG IV) to ensure the exchange of multi-national intelligence and reconnaissance information.

This plan is developed in accordance with current NATO procedures and guidelines under the direction and oversight of the Chairmen of AG IV and the ISR Integration Working Group (ISRIWG). Forward all comments, recommendations, additions, deletions, and other pertinent data that may be of use in improving this document to the ISRIWG Chairman. See the AG IV web page at *http://www.nato.int/structur/AC/224/ag4.htm* for the present ISRIWG Chair's contact information as well as all other points of contact.

1.0 INTRODUCTION

1.0.1 This document defines the basic configuration management principles that shall be applied to the documents under the NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA). This applies to both the STANAGs and Allied Engineering Documentation Publications (AEDPs) that are included in the architecture description of Volume 1. A list of documents included in the NIIA is shown in Volume 1, Annex A of this AEDP.

1.0.2 It is important to maintain the standards and associated documentation in the NIIA document suite in order to ensure that they represent the most current technology and design philosophy. In addition, configuration management is important to ensure that a single version of the document is recognized as current at any given time.

1.1 Background

As the documents that comprise the NIIA have been developed, ad hoc configuration management techniques have been implemented by the Custodians in order to maintain their respective documents. In some cases, the plan was formally published to the community, while in other cases, it was followed by the Custodian without broad user community knowledge of the process. It was recognized by the members of Air Group IV that as the number of documents within the NIIA expanded, some policy guidance should be provided to the Custodians for configuration management. This document was written to provide the top level policy guidance for configuration management for all documents included in the NIIA.

1.2 Reference Documents

1.2.1 Policy and Planning Documents

NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA), AEDP-2

(Copies of the above document can be obtained from the Secretary, AG IV (Air Armaments Section), NATO Headquarters, B-1110 Brussels, BE.)

NATO Standardisation Agreements (STANAG)

STANAG 4545	“NATO Secondary Imagery Format (NSIF)”
STANAG 4559	“NATO Standard Imagery Library Interface (NSILI)”
STANAG 4575	“NATO Advanced Data Storage Interface (NADSI)”
STANAG 4586	“Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability”
STANAG 4607	“NATO Ground Moving Target Indicator Format (GMTIF)”
STANAG 4609	“NATO Digital Motion Imagery Standard”
STANAG 7023	“NATO Primary Image Format (NPIF)”
STANAG 7024	“Air Reconnaissance Tape Recorder Standard”
STANAG 7085	“Interoperable Data Links for Imaging Systems”

(Information on the latest edition/amendment of each STANAG can be found on the AG IV web page. Copies of these STANAGs can be obtained from each nation's Central Registries.)

1.2.3 Other Documents

AAP-3 *Procedures for the Development, Preparation, Production, and the Updating of NATO Standardization Agreements (STANAGs) and Allied Publications (APs)*

1.2.4 Web Page Reference

AG IV Home Page: http://www.nato.int/structur/AC/224/ag4.htm

1.3 Applicability

The NIIA Configuration Management Program is applicable to STANAGs and Allied Publications which document elements of the NIIA. This Configuration Management Program has been defined under the authority of the AG IV Chairman. This Program defines a configuration management framework that may be adopted by Nations, Major NATO Commands (MNC), and NATO organizations responsible for the use, development, configuration management, and implementation of the NIIA.

1.4 Authority

The NATO Conference of National Armaments Directors (CNAD) has directed that subordinate groups shall provide management of the STANAGs and associated documentation for which they have responsibility. AG IV (under the NATO Air Force Armaments Group – NAFAG) manages the STANAGs and related documents through the assignment of Custodians under this direction.

1.5 Requests For Change And Comments On Content

The ISRIWG, on behalf of AG IV, is the configuration management authority for the NIIA. Proposed amendments, with appropriate rationale, should be submitted through the national representatives to the ISRIWG who will submit the changes or comments to the Chairman of the ISRIWG. The change can be submitted using the form included in Appendix 2.

2.0 CONFIGURATION MANAGEMENT PHILOSOPHY

Configuration management is a critical element to maintaining a viable architecture for the ISR community. Without proper configuration management, the standards and associated documentation would quickly become obsolete. As directed by the CNAD and NAFAG, Air Group IV is ultimately responsible for the management of the STANAGs and APs assigned to it. The principles of configuration management for these documents are defined in the following paragraphs.

- Air Group IV will designate a Custodian for each document in the NIIA from individuals proposed by the nations. The sponsoring nation will provide sufficient resources for the Custodians to properly execute their responsibilities defined in this document.

- The focus of the configuration management activities is with the assigned Custodian for each document. Authority for configuration management decisions is vested in the Custodian, with appeals to Air Group IV when necessary.

- Procedures to be used in proposing and processing change requests will be written and available to all users of the documents.

- Changes should be reviewed by the user community to determine the impacts on existing systems and development programs. The configuration management procedures should provide adequate levels of review prior to adoption of proposed changes.

- National representatives to the respective document management board will generally be allowed to review submissions from that nation prior to submission to the entire team for consideration. National reviews are to ensure the proposed change is compatible with national positions.

- When the document is releasable to the general public, the change proposal procedures will include provisions for submission of changes by nationals from non-NATO nations. Specific provisions can be included for submissions by Partners for Peace nationals if deemed appropriate by the Custodian.

- Procedures for processing changes to the documents will be compatible with established processes used by the NATO Standardisation Agency (NSA) for document ratification and promulgation.

2.1 General Configuration Management Processes

There are generally two approaches to managing documents, with multiple variations and combinations of the two concepts. The two concepts relate to the level of formality used to review change proposals. On one side, a lower level on formality allows for faster turn-around of the change requests. However, faster action can result in adoption of proposed changes before a complete assessment of the impacts is complete. A more formal structure generally ensures complete assessments, but generally takes longer to complete.

2.1.1 Formal Configuration Management

The formal configuration management approach allows for complete review of change proposals with a formal appeals process. Figure A-1 shows a nominal flow diagram for the process.

In this figure, (starting at the upper left) the normal process begins with a change request defined and submitted by a user of the standard. The change request is routed to the respective national representative. The national representative can then reject the change proposal, sending it back to the originator with an explanation of why it was rejected, or approve it and forward it to the Custodian. This structure also allows for users in non-NATO nations to submit changes directly to the Custodian. Once received by the Custodian, the administrative support to the Custodian (AST or Administrative Support Team in the figure) logs the change request and can either immediately distribute it for comment or forward it as part of the pre-meeting package prior to the meeting. In this flow diagram, it is the responsibility of the national representatives to distribute the change proposals to the relevant people in their respective nations.

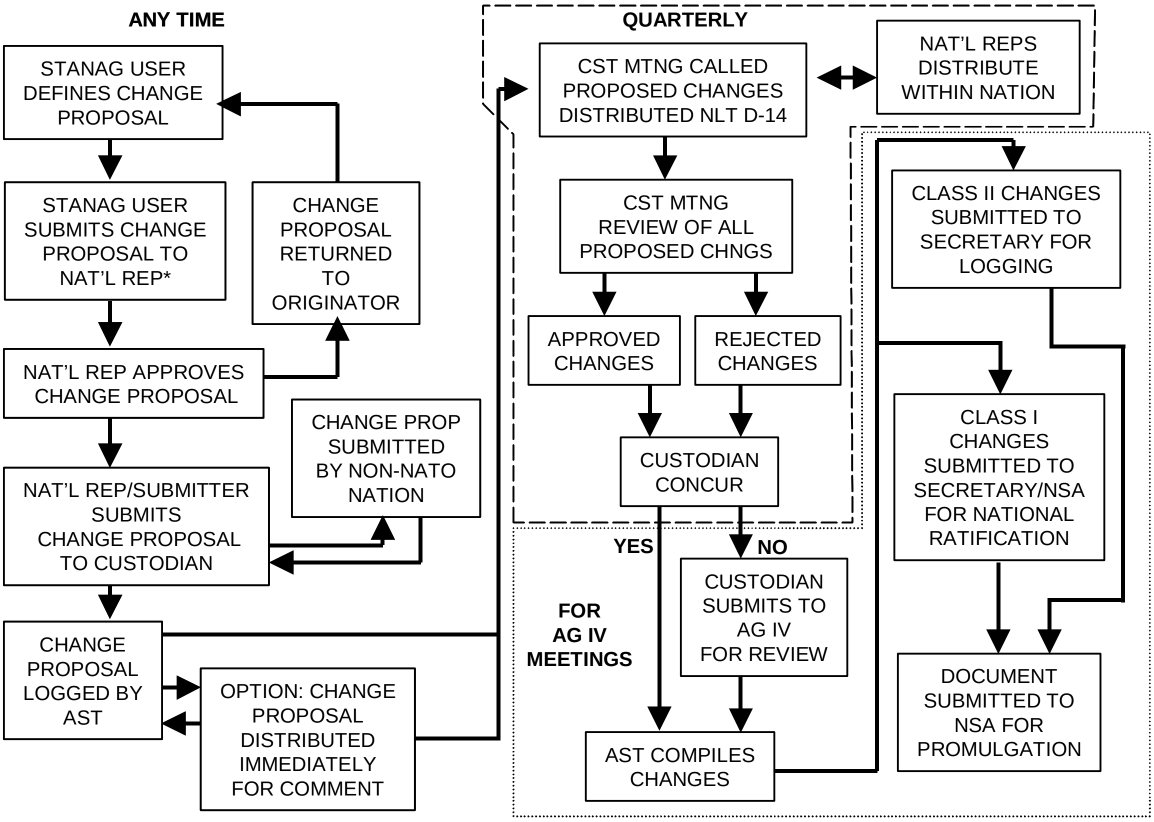
ANY TIME
STANAG USER DEFINES CHANGE PROPOSAL
STANAG USER SUBMITS CHANGE PROPOSAL TO NAT'L REP*
CHANGE PROPOSAL RETURNED TO ORIGINATOR
NAT'L REP APPROVES CHANGE PROPOSAL
CHANGE PROP SUBMITTED BY NON-NATO NATION
NAT'L REP/SUBMITTER SUBMITS CHANGE PROPOSAL TO CUSTODIAN
CHANGE PROPOSAL LOGGED BY AST
OPTION: CHANGE PROPOSAL DISTRIBUTED IMMEDIATELY FOR COMMENT
QUARTERLY
CST MTNG CALLED PROPOSED CHANGES DISTRIBUTED NLT D-14
NAT'L REPS DISTRIBUTE WITHIN NATION
CST MTNG REVIEW OF ALL PROPOSED CHNGS
APPROVED CHANGES
REJECTED CHANGES
CUSTODIAN CONCUR
YES
NO
FOR AG IV MEETINGS
CUSTODIAN SUBMITS TO AG IV FOR REVIEW
AST COMPILES CHANGES
CLASS II CHANGES SUBMITTED TO SECRETARY FOR LOGGING
CLASS I CHANGES SUBMITTED TO SECRETARY/NSA FOR NATIONAL RATIFICATION
DOCUMENT SUBMITTED TO NSA FOR PROMULGATION

FIGURE A-1; FORMAL CM PROCESS FLOW

At the Custodial Support Team (CST) meeting, each change proposal is reviewed and either approved or rejected. With this process flow, the Custodian then has the authority to agree or disagree with the decisions of the CST. If the Custodian does not agree, the issue is passed forward during the Custodian's report to AG IV for final disposition. Once the final change list is completed, the AST compiles the changes. If the changes are editorial, the document is updated and an amendment is issued and provided to NSA for promulgation. Changes with technical content require full ratification by the nations and a ratification draft is forwarded to NSA for formal processing to the nations. Once the ratification process is complete, then the document as a new edition is promulgated.

If issues are not time critical, it mat be appropriate to use a two-meeting cycle, where the change proposals are introduced at one meeting, and then decisions are made at the next.

This process is the most formal procedure and is appropriate when the user community is large and widespread, particularly if multiple nations. It requires only that each national representative have knowledge of the user community within their nation – the Custodian does not have to know of the existence of all of the users. This process allows for the best assessments of impact. It also provides for specific national positions to be considered, both initially to ensure that change proposals are not submitted that are contrary to national positions, and secondarily to have the national representatives distributing the change proposals for review and comment within their respective nation.

2.1.2 Fast Track Procedures

2.1.2.1 The alternate process is one which expedites change proposal processing. In this process, all change proposals are submitted directly to the Custodian, who distributes them to the entire user community. The users then respond with comments and impact statements back to the Custodian. This process is shown in Figure A-2. The basis of this approach is that change requests are processed directly by the Custodian (and/or associated administrative support team). The change requests are then sent directly to all members of the user community. Comments are received and compiled for review by the Custodial Support Team. This review can be done at a formal meeting or via telefax or electronic mail. Once approved, the changes are compiled and depending on the type of change, either submitted to NSA for ratification processing through the nations, or submitted for promulgation of amendments. In this basic approach, change proposals that are not approved are reviewed for concerns and then either adjusted or withdrawn. In a sense, no proposal is actually rejected.

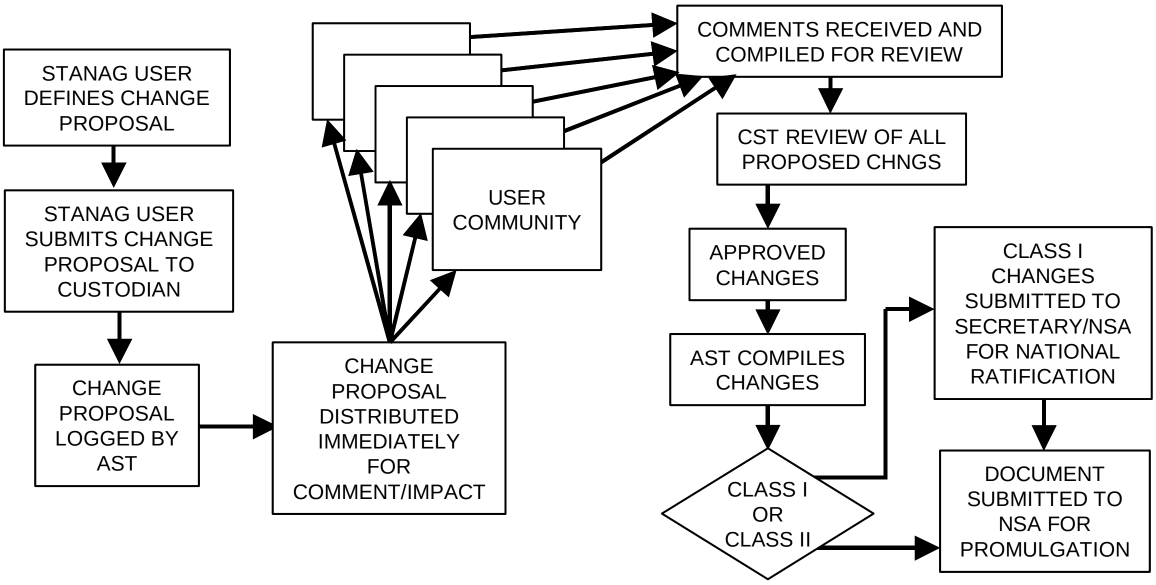
STANAG USER DEFINES CHANGE PROPOSAL
STANAG USER SUBMITS CHANGE PROPOSAL TO CUSTODIAN
CHANGE PROPOSAL LOGGED BY AST
CHANGE PROPOSAL DISTRIBUTED IMMEDIATELY FOR COMMENT/IMPACT
USER COMMUNITY
COMMENTS RECEIVED AND COMPILED FOR REVIEW
CST REVIEW OF ALL PROPOSED CHNGS
APPROVED CHANGES
AST COMPILES CHANGES
CLASS I OR CLASS II
CLASS I CHANGES SUBMITTED TO SECRETARY/NSA FOR NATIONAL RATIFICATION
DOCUMENT SUBMITTED TO NSA FOR PROMULGATION

FIGURE A-2; FAST TRACK CM PROCESS FLOW

2.1.2.2 The key to success with this process is that the user community must be relatively small and the Custodian must know who the key users are. Because of the time-critical approach, allowing fast change, the risk is that impacts may not be totally understood prior to making decisions on the proposals. If a key member of the user community is not included on the distribution of the change proposal, that input will not be considered and the change could have a major impact on the respective system or program. The worst-case scenario would be to have a member of the user community not involved and then when a change is adopted, the uninvolved user would not adopt the change and multiple versions of the standard would then be used in systems. This would quickly negate all of the benefits of the interoperability standards in the NIIA.

2.1.3 Combinations Of Management Techniques

A number of variations on these techniques are possible, combining both processes into a single flow diagram. Variations on the formal process can include a fast track line for specific types of changes, for example, editorial changes, or changes to a specific feature of the standard used only by specific users. Variations on the fast track approach can include formal rejection of unacceptable proposals, an appeal process for rejected proposals, and Custodian review of the process.

2.2 Configuration Management Plans

2.2.1 The Custodian of NIIA documentation shall prepare a configuration management plan, documenting how change proposals will be submitted, adjudicated, and disposed of. The plan will include the responsibilities of the Custodian, define specific support planned from administrative support, define the membership and procedures of the Custodial Support Team, and provide specific instructions on how to submit requests for change.

2.2.2 The Custodian will present the configuration management plan to Air Group IV as part of the normal reporting during the AG IV meeting. AG IV will accept or reject the plan, and if rejected, will identify the reasons for the rejection so that the Custodian can correct the plan for future AG IV approval. The Custodian will also identify how the plan will be published, either as a stand-alone document or as part of other associated documentation. Regardless of the form of publication, the ISRIWG Chairman will ensure that the formal references to the plan are incorporated into the list of documents that make up the NIIA.

3.0 CONFIGURATION MANAGEMENT ISSUES

There are a number of specific issues that should be considered by Custodians in the development and publication of configuration management plans.

3.1 Change Classes and Standard Revisions

3.1.1 In accordance with AAP-3, changes to NATO STANAGs are defined in one of two classes. Class I changes are those that are substantive in nature and involve technical changes to the standard’s requirements. Generally, any change that would impact the design or implementation of the standard in a system is a Class I change. Class I changes require that the document be processed as a new edition of the STANAG and be submitted to the nations for formal ratification, just as the original STANAG was processed. The ratification process through the nations can take over a year, so the Custodian should be prepared to accommodate the schedule requirements of this extensive process.

3.3.2 Class II changes are those that are to correct editorial errors or clarify a requirement without making specific changes to it. Class II changes are approved by the Custodian and do not require re-ratification. Class II changes should be briefed by the Custodian to AG IV during the Custodian's normal report to allow discussion and comment prior to promulgation. Then, once the Class II change is complete, it is submitted through the AG IV Secretary to the NSA for promulgation. Class II changes result in an amendment to the current edition.

3.2 Document Definitions

3.2.1 Changes to documents are defined in AAP-3 based on the stage of activity of the document. Figure A-3 shows a notional sequence of a standard as it is developed and changed during its lifetime. The document starts as a study draft. The management of the study draft is performed by using version numbering, date/time groups, or any other technique acceptable to the study team. The notional document is produced in two versions before the team creates the ratification draft (normally, a standard will go through many more iterations before creation of the ratification draft). If it is determined that the original approach to the standard was incorrect, the entire document can be discarded and Edition 1, Study Draft 2 could be created (this is not shown in the figure). With the creation of ratification draft 1, the document is distributed to the nations for ratification. The approved document then becomes Edition 1, and is promulgated by NSA.

3.2.2 In this notional sequence, the next event is the definition of some editorial changes. Frequently this is required since typographical errors or sections that are unclear to the user community (particularly those not involved in the creation of the document) will be identified once the document is release for use. The editorial changes are approved by the Custodian and used to generate Edition 1, Amendment 1. This document is provided to NSA for promulgation.

3.2.3 The next change is identified as a technical change, requiring national ratification. The first ratification draft of Edition 2 is sent to the nations, and for some reason, the document is not approved. The necessary changes are incorporated, and Ratification Draft 2 of Edition 2 is prepared and submitted to the nations for ratification. This version is ratified by the nations and Edition 2 is then promulgated by NSA.

3.2.4 The final line of the notional sequence is the identification of a requirement to completely change the standard. A study draft for Edition 3 is prepared as was done for the original document. This study draft progresses through to a ratification draft, and ultimate will be Edition 3 if ratified by the nations

3.2.5 It should be noted that while amendments are officially approved by the Custodian, Air Group IV expects to be briefed on amendments prior to submission to NSA for promulgation. New editions require full ratification by the nations.

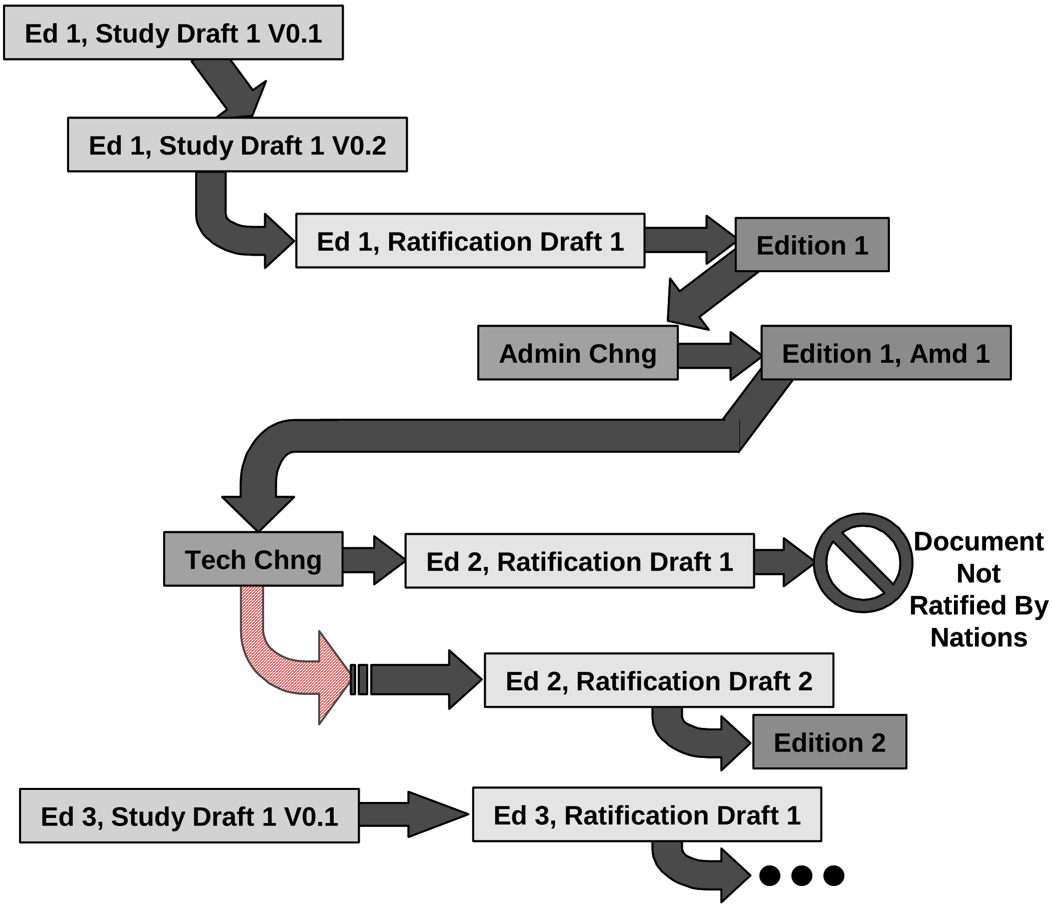
Ed 1, Study Draft 1 V0.1
Ed 1, Study Draft 1 V0.2
Ed 1, Ratification Draft 1
Edition 1
Admin Chng
Edition 1, Amd 1
Tech Chng
Ed 2, Ratification Draft 1
Document Not Ratified By Nations
Ed 2, Ratification Draft 2
Edition 2
Ed 3, Study Draft 1 V0.1
Ed 3, Ratification Draft 1

FIGURE A-3; NOTIONAL NATO DOCUMENT REVISIONS

3.3 Allied Publication Processing

3.3.1 The NIIA (including this document) is documented in a number of STANAGs and Allied Publications. In particular, the Allied Engineering Documentation Publication (AEDP) is used to provide both the top level description and guidance on the NIIA, as well as specific guidance on the implementation of the different STANAGs. The AEDPs will also have Custodians. Generally, the Custodian of the STANAG-related AEDPs will be the Custodian of the related STANAG.

3.3.2 When processing AEDPs, the Custodian will follow similar processes as those defined for the STANAGs. The significant difference in the processing of APs is that they do not require national ratification. APs require approval of the tasking authority. In the case of the NIIA, this is Air Group IV. Once the ratification draft of an AEDP is complete, it is presented to AG IV for approval (ratification), and then submitted through the Secretary to NSA for promulgation.

3.3.3 When processing change proposals for the AEDPs, the process follows the same guidelines as for STANAGs, with Class II changes being approved by the Custodian (and briefed to AG IV), and Class I changes ratified by AG IV directly

3.4 Errata Sheets

3.4.1 One alternative for processing change requests is to use an Errata Sheet. An Errata Sheet defines proposed changes that have been approved for incorporation into the next iteration of the document, but is not extensive enough to warrant a change at this time. Errata Sheets advise developers and others in the user community that the changes will be incorporated into the next iteration of the document, but have not in the current release. While it is not mandatory that the user community adheres to the Errata Sheet, they would be advised to, since the changes will be coming and compliant systems will be eventually tested against the standard with the changes incorporated.

3.4.2 It is important that if the Errata Sheet approach is used, that it is available to the entire user community, and it is readily recognizable that the Errata Sheet has been published against a particular version of a document. Publishing an Errata Sheet and then not properly distributing it, negates the entire concept of the Errata Sheet. It can be distributed through national representatives to the respective CST, through the AG IV representatives, directly to known user community representatives, and/or on the NATO web page (particularly if the STANAG is also available on the web).

4.0 BACKWARD COMPATIBILTY

During the necessary process of further developing existing STANAGs, backward compatibility between following editions of the same STANAG should be considered a main objective. Backward compatibility secures NATO and national investments. The prospect of a considerably altered and probably widely incompatible new edition of the same STANAG might adversely affect acceptance and delay or hinder necessary decisions or further investments in this STANAG.

4.1 Baseline

In general, changes to a STANAG that alter structure and concept of core segments or data structures should be executed generally reluctant and only after reasonable efforts have been taken to check possible alternatives.

4.2 Backward Compatibility Criteria

The following backward compatibility criteria may be used to aid discussion of this issue. A follow-on edition of the same STANAG may be considered backward compatible to the previous one, if:

- The follow-on edition contains the previous edition as an unaltered subset;Data prepared according to a previous edition can be used by a system designed for the follow-on edition without modification;
- The intended purpose of the same segments or data structures is not altered between editions;
- Skipping or ignoring of new segments or data structures of a follow-on edition leads to valid data according to the previous edition;Systems designed for previous versions can identify newly formatted data and ignore new features; and

- Data that are valid according to a previous edition are valid data in the follow-on edition as well.

4.3 Backward Compatibility Policy

4.3.1 Backward compatibility of all NIIA STANAGs is generally required. NIIA STANAG Custodians are to identify to the ISRIWG any new capabilities that they intend to incorporate into their respective STANAG, before implementing them. In addition, the Custodian will notify the ISRIWG if new planned capability is not backward compatible. The Custodian will provide a cost-benefit trade analysis and explain why the lack of backward compatibility is desirable. The ISRIWG will establish a position on the proposal and present it to AG IV with the Custodian for a final decision.

4.3.2 It is recognized that totally new capabilities (e.g. XML) are a major change and will not necessarily be backward compatible with existing protocols. The Chairman of the team developing the new capability will identify it to the ISRIWG. The ISRIWG will incorporate the new capability into the NIIA. However, once established, the new capability should adhere to the backward compatibility philosophy identified above

5.0 CONCLUSIONS

The policy document provides guidance to Custodians of the NIIA documents on how to manage their documents, and review and incorporate proposed changes into their document. While this document does not prescribe a specific plan for all to use, leaving the details of the configuration management plan to the respective Custodians, this document does provide general guidelines and options for the configuration management approach.

GLOSSARY

Acronym

AEDP	Allied Engineering Documentation Publication
AG IV	Air Group IV (under CNAD/NAFAG)
AP	Allied Publication
AST	Administrative Support Team
ATTN	Attention
BE	Belgium
CM	Configuration Management
CNAD	Conference of National Armaments Directors
COTS	Commercial Off-The-Shelf
CST	Custodial Support Team
HQ	Headquarters
IEC	International Electrotechnical Commission
ISO	International Organization of Standardization
ISR	Intelligence, Surveillance, and Reconnaissance
ISRIWG	ISR Integration Working Group (under AG IV)
MNC	Major NATO Commands
NAFAG	NATO Air Force Armaments Group (under CNAD)
NATO	North Atlantic Treaty Organization
NIE	NATO Interoperability Environment
NIETWG	NATO Interoperability Environment Testing Working Group
NIIA	NATO ISR Interoperability Architecture
NIMP	NATO Interoperability Management Plan
NSA	NATO Standardisation Agency
POC	Point(s) of Contact
STANAG	Standardization Agreement
TBD	To Be Determined

Term	
Administrative Support Team	The Group tasked within the configuration management plan to support the Custodian by performing the administrative tasks associate with the management of the publication
Amendment	In STANAG terminology, this defines each release of the STANAG (or AP) that incorporates only editorial or clarification changes
Class I	The type of change that incorporate significant or technical changes to the requirements of the STANAG (see AAP-3)
Class II	The type of change that incorporates only editorial or clarification changes (see AAP-3)
Custodial Support Team	The Group tasked within the configuration management plan to make the decisions on the proposed changes
Edition	In STANAG terminology, this defines each release of the STANAG (or AP) that incorporate significant or technical changes to the requirements of the STANAG
Errata Sheet	A change control technique that allows changes to be compiled as approved and published for the user community without a formal change to the document. Generally, changes are added to the errata sheet until sufficient changes are approved to warrant a revision to the document.
promulgation	the process of formally distributing a NATO publication and incorporating the document into the official register of documents (see AAP-3)
ratification	the process of approving a NATO publication, for STANAGs, by submission to the individual nations (see AAP-3)

CHANGE REQUEST FORM
STANDARDIZATION DOCUMENT CHANGE PROPOSAL

INSTRUCTIONS

1. Change proposals may be submitted on this form through either mail or telefax, or by electronic mail following the same order and content as this form.
2. Originator completes sections 1-16.
3. Originator forwards to the respective national representative to the ISRIWG. If none exists from the originator's nation, then the representative to Air Group IV shall be the recepient. (See the NATO NAFAG AG IV Internet web page for names and addresses.)
4. National representative approves or rejects proposal from their nation by completing sections 17-25.
   - Approved proposals are forwarded to the Chairman of the ISRIWG.
   - Rejected proposals are annotated with the reason for disapproval and returned to the originator.

Note: This form may be used to submit changes to the NIIA Test and Evaluation Program Plan. This form may not be used to request copies of this documents. The document is available on the NATO NAFAG AG IV Internet home page (www.nato.int/structur/AC/224/home.htm), or through normal NATO document distribution channels.

RECOMMENDED CHANGE: (continue on additional sheets as necessary) page | | of | |

1. Document Number:

2. Document Version/Release Number:

3. Document Date:

4. Document Title:
NATO ISR Interoperability Architecture (NIIA) Test and Evaluation Program Plan

5. Proposed Change to: (Section, Paragraph, Line, Page)
|

6. Change Class: I| | II |
| | | |

7. Current Wording:

8. Proposed Wording:

9. Reason/Rationale:

10. Originator's Name:

13. Originator's Telephone Number:

11. Originator's Organization:

14. Originator's Telefax Number:

12. Originator's Mailing Address:

15. Originator's E-Mail Address:

16. Date Submitted:

17. Nat'l Rep Name:

20. Nat'l Rep Telephone Number:

18. Nat'l Rep Organization:

21. Nat'l Rep Telefax Number:

19. Nat'l Rep Mailing Address:

22. Nat'l Rep E-Mail Address:

23. Date of Approval/Rejection:

24. Change Proposal: Approved |___| Rejected: |___|

25. Rejection Rationale:

Mail, Telefax, or E-Mail Change Proposals To:
ISRIWG Chairman

26. Date Logged by ISRIWG/initials:

FOREWORD

This plan describes the North Atlantic Treaty Organization (NATO) Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA) Test and Evaluation Program. The NIIA defines the architecture for exchanging digital ISR data between NATO nations. The NIIA consists of a suite of standards that are assembled under NATO Air Group IV (AG IV) to ensure the exchange of multi-national intelligence and reconnaissance information.

This plan is developed in accordance with current NATO procedures and guidelines under the direction and oversight of the Chairmen of AG IV and the ISR Integration Working Group (ISRIWG). Forward all comments, recommendations, additions, deletions, and other pertinent data that may be of use in improving this document to the ISRIWG Chairman. See the AG IV web page at *http://www.nato.int/structur/AC/224/ag4.htm* for the present ISRIWG Chair's contact information as well as all other points of contact.

1.0 INTRODUCTION

1.1 Purpose

This document establishes the North Atlantic Treaty Organization (NATO) Intelligence, Surveillance and Reconnaissance (ISR) Interoperability Architecture (NIIA) Test and Evaluation Program for achieving and sustaining NIIA data compliance by ISR systems. It describes the processes, procedures, and policy to arrange NIIA compliance testing for an ISR implementation.

1.2 Objectives

The overall objective of the NIIA Test and Evaluation Program Plan is to outline the process, procedures, and policy for NIIA testing activities of NATO owned and national ISR systems, by:

- Ensuring early identification of testing requirements to allow all participants to obtain the resources necessary to adequately participate in the testing program.
- Ensuring that similar NIIA testing requirements are identified to allow consolidation of requirements, where feasible, and allow for more efficient use of testing resources.
- Ensuring that NIIA testing requirements are prioritized in accordance with guidance provided by Air Group IV (AG IV) and the ISRIWG.
- Provide coordination with the NATO Interoperability Environment (NIE) Testing Working Group (NIETWG).

1.3 Scope

This Program Plan addresses the NIIA Test and Evaluation Program, policies and procedures, roles and responsibilities, test-funding guidance, facilities, and registration. The plan also establishes test and certification guidance to the NIIA Custodians and establishes the linkage to the NATO Interoperability Environment (NIE) Testing Concept. Standard validation testing and standards compliance testing is managed by the Custodian of the respective STANAG. Interoperability testing and demonstrations are managed by the Demonstration Team under the ISR Integration Working Group (ISRIWG) under AG IV.

1.4 Background

NATO recognized a need for improved interoperability between NATO-owned assets as well as individual nations' ISR systems. As a result, the NATO ISR Interoperability Architecture was created by a technical team under the direction of NATO AG IV. This architecture provides guidance for the exchange of ISR data between NATO nations. The resulting architecture is documented in Standardisation Agreements (STANAGs) and related Allied Engineering Documentation Publications (AEDPs).

1.5 References

1.5.1 Policy and Planning Documents

- NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA), AEDP-2
- NATO Interoperability Management Plan (NIMP), Volume II, AC/322-D/26
- NIE Testing Concept, AC/322(SC/2-WG/3)N/133
- Rolling NATO Interoperability Environment (NIE) Test Programme (RNIETP), Annex 1 to AC/322 (SC/2-WG/3)M/53, 23 April 2001, Version 1.1

(Copies of the above document can be obtained from the Secretary, AG IV (Air Armaments Section), or the Secretary, ISC (NHQC3S/IOB), NATO Headquarters, B-1110 Brussels, BE.)

1.5.2 Other Documents

- ISO/IEC 10641, Information Technology – Computer Graphics and Image Processing – Conformance Testing of Implementations of Graphics Standard, First Edition, 1993.

1.5.3 Web Page Reference

AG IV Home Page: http://www.nato.int/structur/AC/224/ag4.htm

1.6 Applicability

1.6.1 The NIIA Testing Program is applicable to testing performed during the development, configuration management, implementation, and operational use of NIIA to ensure its successful implementation in ISR systems. This Program Plan has been defined under the authority of the AG IV Chairman. This Program Plan defines a testing framework that may be adopted by Nations, Major NATO Commands (MNC), and NATO organizations responsible for the use, development, configuration management, and implementation of the NIIA.

1.6.2 Industries, which develop commercial-off-the-shelf (COTS) systems that implement the NIIA, are recommended to submit their products for testing under the provisions of this Test and Evaluation Program Plan. NATO and nations that acquire COTS to use in their ISR systems should insist on tested products.

1.7 Authority

The NATO Conference of National Armaments Directors (CNAD) has directed that subordinate groups shall provide management of the STANAGs and associated documentation for which they have responsibility. AG IV (under the NATO Air Force Armaments Group – NAFAG) manages the STANAGs and related documents through the assignment of Custodians under this direction.

1.8 Test Sponsorship

A Test Sponsor is any individual or organization interested in acquiring or providing funding for the purpose of testing an implementation of a standard. The Test Sponsor shall be the focal point for coordinating the testing from the implementation development side. There are three sources of test sponsorship. The three different sources require different approaches to sponsoring and paying for the testing activities. The three sources are NATO government sponsored, commercially sponsored, and non-NATO government sponsored tests. Requests for testing should be addressed to the Test Facility point of contact (POC) following the general procedures outlined in this plan and the detailed instructions for each test facility include in the web site. Specific procedures will vary based on the STANAG to be tested, the facility performing the tests, and the nations involved. Specific procedures can be found in the web page for the specific STANAG and participants must adhere to the guidelines provided.

2.0 NIIA TEST PROGRAM

The NIIA Test and Evaluation Program encompasses all aspects required to achieve and sustain NIIA interoperability, including the administrative bodies (including the test facilities), policies, and procedures. The NIIA Test and Evaluation Program supports NATO objectives to ensure interoperable systems for coalition operations.

2.1 Test Program Concept

2.1.1 This program is designed to provide the level of testing necessary to provide an increased level of confidence that systems allocated to a coalition operation will be interoperable. There are three types of testing included in the test concept. They are document validation, compliance tests, and interoperability tests. Document validation is the verification that the standard is complete and understandable, and meets the agreed features or requirements. Compliance tests provide a way of scrutinizing implementations of a STANAG to determine whether or not deviations from the STANAG exist. Interoperability tests typically take the form of demonstrations and show that two or more independent implementations work properly together. The last two, compliance tests and interoperability tests, are often used together in an iterative fashion to verify that the compliance tests are complete and accurate – testing the right functionality in the right way – while providing confidence that implementations certified as compliant are interoperable as well. Validation and compliance tests are managed by the respective Custodian. Interoperability tests frequently involve more than one STANAG, and therefore will be managed by the ISRIWG.

2.1.2 NIIA testing is essential to ensure that current and future systems or system components implementing NIIA standards and products will interoperate effectively under a variety of conditions. Compliance and interoperability testing are complimentary types of testing. Compliance testing is more technically oriented, whereas interoperability testing is closer to the operational environment. Compliance testing increases the probability that multi-system implementations of NIIA standards will interoperate, but does not assure their interoperability. Compliance testing cannot ensure that the behavior of the implementation will be consistent once in the operational environment. To provide a level of assurance of interoperability of NIIA standards implementation, interoperability testing is also required.

2.1.3 The concept of this Test Program Plan is to provide flexibility and adaptability to the tests conducted for each STANAG. Testing should be selected to provide a high level of confidence that implementations will be interoperable. All testing has risks, and tests should be selected to minimize risk to future coalition operations, while balanced against the resources required to perform the tests.

2.1.4 While this Test Program Plan identifies the top-level policies and procedures for NIIA testing, specific test criteria and procedures for the testing of each STANAG are identified elsewhere. Consult the information included in the AG IV home page for each STANAG for the test criteria and the test facilities involved for further information on the test procedures.

2.1.5 This Test and Evaluation Program provides for the establishment and accreditation of multiple test facilities for each STANAG. In cases where more than one facility is accredited to test a specific STANAG, a lead facility should be designated.

2.2 NIIA Test And Evaluation Program Test Policies & Procedures

The following policies are aspects of the NIIA Test and Evaluation Program.

2.2.1 Compliance Policy

In order for systems (hardware and/or software) to be listed in the applicable registry, it must demonstrate its compliance with the specific STANAG through testing, in accordance with the guidelines specified by the Custodian. Compliance to specific standards is at the discretion of the nations, but all nations are encouraged to provide interoperable systems when operating in coalition environments, and mandate the standards identified in the NIIA during their acquisition programs. Agreement to comply with specific STANAGs is identified in the ratification page of the respective STANAG.

2.2.2 Test Location

Compliance testing will be conducted at the accredited NIIA Test Facility or at an agreed-upon location on a case-by-case basis.

2.2.3 Testing Policies

The tests conducted under this program will be in accordance with the following guidelines:

- All testing will be conducted by accredited test facilities. The Custodian will accredit test facilities for the specific STANAG.
- Costs for testing may be reimbursable and can be negotiated among the participants.

2.2.3.1 Document Validation Test Policies

The following policies apply to tests conducted to validate standards and changes to standards:

- The Custodian will determine the standard validation activities required for the STANAG and will be responsible for managing the validation tests.
- Validation of technical changes to STANAGs should be considered prior to adoption of the change.
- Editorial changes do not normally require validation.

2.2.3.2 Compliance Test Policies

The principal purpose of compliance testing is to assess the degree to which the external behavior of a system or implementation conforms to the NIIA standard. An implementation can be understood as a system, system component (hardware and/or software), or product under test. The principal benefit of compliance testing is that the performance of each implementation under test is tested in an isolated situation against a validated standard, allowing for identification of implementation failures, and standards/specification violations. The following policies apply to tests conducted to verify compliance with specific standards:

- The Custodian is responsible for managing their respective STANAG compliance testing.
- All tests will be conducted by accredited, independent organizations with no vested interest in the successful completion of the tests.
- Tests will be conducted using predefined test criteria and procedures available to all parties.
- A record of discrepancies will be provided to the test sponsor and developer and will be maintained by the test facility for future reference. This record will include, as a minimum, a detailed description of the discrepancy, the impact of the discrepancy on the user community and interoperability, and a recommendation on resolution.
- A test report will be generated which documents the tests conducted, the discrepancies found and the status of each, and the specific implementation tested.
- All successfully completed tests to be entered into the registry will be identified to the respective Custodian.

2.2.3.3 Interoperability Test Policies

Interoperability testing assesses the operations of an implementation with systems performing the same or complementary operational functions. Interoperability testing is an evaluation that assesses the overall capability and behavior of a complete system in an operational environment using live and/or simulated or theoretical data, in a fielded testing environment, or in a developmental environment. The following policies apply to tests conducted to demonstrate interoperability:

- Interoperability tests and demonstrations will be managed by the ISRIWG.
- The ISRIWG Chairman will identify a test manager for interoperability tests and demonstrations.
- Participating nations will provide national resources to the demonstration team to execute the interoperability tests and demonstrations.
- Tests will be conducted using predefined test criteria and procedures available to all parties.
- A record of discrepancies will be provided to the test sponsor and developer and will be maintained by the ISRIWG for future reference.
- A final test report will be produced and provide to all participants.

2.2.4 Retesting Policy

The NIIA Custodian may direct implementation compliance retesting. Sponsors and/or developers may also request implementation retesting under conditions such as the following:

- A final test report will be produced and provide to all participants.
- Changes to the NIIA standard compliance requirements
- Latent functional problems discovered with previously tested implementations
- Any changes to a configuration controlled item of a NIIA compliance tested implementation
- The period for registration has elapsed

2.3 Test Program Responsibilities

Figure B-1 depicts these organisational relationships. The relationship between the NIIA Test Customer and the NIIA Test Facility is established on a case-by-case basis. Typically it will be documented in a Memorandum of Understanding.

The following paragraphs describe the responsibilities of principal organizations that assist in implementing the NIIA Test Program.

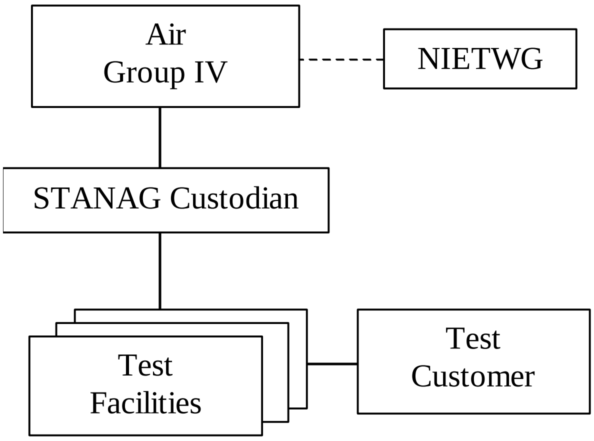

Figure B-1 - NIIA Test Program Organisational Relationships

2.3.1 Air Group IV (AG IV)

The AG IV Chairman has the responsibility and authority for the development and configuration management of the NIIA. AG IV oversees NIIA testing through the NIIA Test and Evaluation Program. AG IV appoints the STANAG Custodian. AG IV will also serve as the final arbitrator of issues between STANAG Custodians and other NIIA Test and Evaluation Program participants.

2.3.2 NIIA STANAG Custodian

The STANAG Custodian is the delegated NATO authority for the management oversight of the specific STANAG. There is a close relationship between configuration management and testing of a specific STANAG. Therefore, the custodian shall be responsible for the day-to-day oversight of the STANAG validation and compliance testing activities and also have responsibility for maintaining configuration control of the STANAG.

The STANAG Custodian has the following responsibilities:

- Defines the testing program applicable to the specific STANAG. The Custodian can choose to implement all or part of the testing defined in this Test Program Plan, and can add additional elements of test as necessary.
- Presents the testing structure for the STANAG to the ISRIWG and AG IV for approval.
- Produces and maintains the compliance test criteria documentation for the respective

STANAG.

- Arbitrates any testing issues from validation or compliance testing.
- Assists in resolving functional and interoperability problems with NIIA compliant implementations.
- Coordinates the testing activities with the STANAG configuration management.
- Resolves STANAG issues presented during development, validation, implementation, testing, and operations that impact ISR system interoperability.
- Assists to resolve test issues that surface during interoperability testing and demonstrations.
- Reviews STANAG testing facilities' procedures, testing, and compliance registration process.
- Approves accreditation of respective STANAG Test Facilities.
- Provides response to test facility with rationale if disapproved for accreditation.
- Designates a lead test facility, if necessary.
- Approves/disapproves test facility compliance recommendations.
- Publishes and maintains a master register of compliant systems, implementations, and components on the NATO web site.
- Works with other Custodians and the ISRIWG Chairman to resolve issues that arise between the STANAGs.
- Review and approve or disapprove compliance test plans.
- Review completed compliance test reports and approve/disapprove the inclusion of a tested system on the master register of compliant systems.
- Notify the Test Sponsor of the outcome of the Custodian's review of the test report, and provide guidance on items to be corrected on unsatisfactory reports.
- Notify the Test Sponsor, system developer or National Sponsor when retesting of a system becomes necessary for any of the reasons cited in paragraph 2.2.4.

2.3.3 ISRIWG Chairman

2.3.3.1 The ISRIWG Chairman is the delegated authority for the management of activities and issues associated with multiple STANAGs. The ISRIWG Chairman will coordinate testing schedules for interoperability tests and demonstrations with the NIETWG. The NIETWG will add the NIIA test activities to the master testing schedule.

2.3.3.2 The ISRIWG Chairman has the following responsibilities:

- Manages interoperability tests and demonstrations.
- Arbitrates any testing issues from interoperability testing.
- Assists in resolving functional and interoperability problems with NIIA compliant implementations.
- Resolves NIIA issues presented during STANAG development, validation, implementation, and interoperability testing that impact ISR system interoperability.
- Publishes and maintains a register of interoperability test and demonstration results on the AG IV web site.
- Resolves issues that arise between the STANAGs.
- Coordinates interoperability testing and demonstration schedules with the NIETWG.
- Reports interoperability test and demonstration results to the NIETWG.
- Coordinates interoperability test and demonstration planning, scheduling, and execution.

2.3.4 NIIA Test Facilities

2.3.4.1 The Test Facilities encompass the facilities, hardware, software, and personnel that support validation and compliance testing of NIIA capable implementations. Each NIIA Test Facility has the following responsibilities:

- Establishes, manages, and operates the certification test facility.
- Maintains knowledge, skill, and proficiency of test personnel.
- Validates/revalidates STANAG as originally written and then as changes are implemented.
- Plans, schedules, and executes compliance tests.
- Supports interoperability tests and demonstrations.
- Processes test and retest requests.
- Arbitrates test-scheduling conflicts in coordination with the STANAG Custodian.
- Publishes compliance test results and recommends certification.
- Advises the STANAG Custodian regarding test program issues and forward recommendations regarding certification.
- Mutually coordinates with other NIIA Test Facilities to ensure consistency of testing.
- Maintains the certification test procedures.

2.3.4.2 In addition to the above responsibilities, when a facility is designated as a lead test facility, the following responsibilities also apply:

- Participates in the review of applications for accreditation by potential test facilities.
- Provides assistance to other test facilities to ensure consistency of tests.
- Ensures that test procedures developed by other facilities meet the test criteria for the STANAG.
- Periodically reviews test procedures and activities of other facilities to verify compliance with test criteria and guidelines.
- Maintains the certification test criteria.

2.3.5 Test Sponsor

A test sponsor has the following responsibilities:

- Submits requests testing for compliance certification.
- Coordinates with the developer to request NIIA compliance testing and/or retesting.
- Assists in coordinating international agreements, test license agreements, purchase orders, and terms and conditions for testing agreements (as needed) to accomplish compliance testing.
- Provides primary and alternate points of contact for compliance testing matters.
- Programs and budgets for the direct NIIA compliance testing costs, plus the associated manpower, equipment, shipping, travel, and per-diem costs.

2.3.6 Implementation Developer

2.3.6.1 The NIIA Implementation Developer may in some cases be the same as the Test Sponsor. The Implementation Developer may be a government or commercial entity. Procedures may vary for Implementation Developer depending on whether they are from the same nation as the test facility. Refer to the web pages for each STANAG listing the particular test facilities for specific instructions on test procedures.

2.3.6.2 An Implementation Developer has the following responsibilities:

- Promptly reports functional problems experienced with NIIA tested configuration items to the NIIA Test Facility.
- Provides the test facility the necessary information to accomplish testing.
- Provides technical support to answer questions and make modification as required.

2.3.7 ISRIWG Demonstration Teams

The ISRIWG Demonstration Teams are organized under the terms of the ISRIWG Work Plan to manage interoperability tests and demonstrations. The Demonstration Teams are led by respective Demonstration Team leaders, who are appointed by the ISRIWG Chairman. The Demonstration Teams have the following responsibilities:

- Develops the demonstration roadmap supporting the NIIA interoperability goals.
- Establishes short term milestones for meeting roadmap goals.
- Develops interoperability/demonstration architecture based on system availability and maturity.
- Defines test concepts, criteria, and plans for interoperability tests and demonstrations.
- Manages the interoperability tests and demonstrations.
- Analyze the data collected during interoperability tests and demonstration.
- Produces test reports for interoperability tests and demonstrations.

2.4 Test Program Resources

2.4.1 Introduction

Before testing, as part of the test preparation, resources to execute NIIA testing have to be identified and secured by the Testing Sponsor. Resources will include funding, manpower, equipment, and possibly a facility to conduct the test.

2.4.2 Funding

Based on the test objectives and evaluation criteria, a test facility will prepare a cost estimate to plan, conduct, and report on the test. In principle the Testing Sponsor is responsible for securing the funding for a test, but does not necessarily have to provide the funds. An example could be a national project office acting as a Test Sponsor with a vendor providing funding for the test.

2.4.3 Resources Required for NIIA Custodian Activities

To ensure that the Custodian responsibilities are properly carried out, the nation providing the Custodian shall ensure that resources are made available as required. Other NATO nations are encouraged to actively participate in the Custodial Support Teams to review proposed changes to the STANAGs.

2.5 NIETWG Coordination

This program will be coordinated with the NIETWG through a liaison agreement. Testing will be conducted under the direction of AG IV, the ISRIWG, and the STANAG Custodians. However, schedules for interoperability tests and demonstrations will be provided to the NIETWG by the ISRIWG Chairman for incorporation into the master planning schedule.

2.6 Points Of Contact

2.6.1 NATO AG IV NIIA Test Oversight

Air Group IV Secretary
ATTN: Mr. Georges L. Thibaut
Air Armaments Section
NATO HQ
1110 Brussels, Belgium
Phone: 32-2-7070-4288
Fax: 32-2-707-4103

2.6.2 STANAG Custodians

The Custodians for each STANAG are listed on the AG IV web page as noted in paragraph 1.4.4. Names and email addresses are available and current. Contact the individuals shown for further information on the STANAG(s) of interest.

2.6.3 NIETWG Coordination

NHQC3S/IOB
NATO Headquarters
B-1110 Brussels
Attn: Secretary, ISC
Email: isc@hq.nato.int

3.0 STANDARDS DOCUMENT VALIDATION TESTING

3.1 General

Document validation is performed for new standards and for technical changes to existing STANAGs. Editorial changes do not require validation testing unless directed by the Custodian.

3.1.1 Initial Validation Testing

Initial validation testing is used to ensure that the draft document is complete and accurate prior to release for ratification and promulgation. The Custodian will determine the scope of the initial validation testing required.

3.1.2 STANAG Change Validation Testing

As changes or additions are nominated to a STANAG, they can be validated, if determined necessary by the Custodian, through testing, prior to Custodial Team approval for incorporation into the STANAG. These tests would be used to ensure that the changes or additions are technically correct, consistent, complete, and testable. In addition, changes to the compliance requirements of the respective Test Criteria/Procedures may be required. Refer to the applicable Configuration Management Plan for guidance in proposing changes to a STANAG.

3.1.3 Validation Testing Methodology

The process for validating a proposed STANAG or change to an existing STANAG is as follows:

- Step 1: The nation, service, functional, and/or performance requirements are fully identified and an appropriate authority ratifies that the requirements are valid.
- Step 2: As the proposed standard or change is written, compliance test objectives, criteria, and test cases are also written that will be used to ascertain whether the proposed solution satisfies the validated requirements.
- Step 3: A sample implementation of the proposed standard or change should be implemented. The test procedures and tools needed to conduct compliance testing should also be developed independently of the developer, but in synchronization with the development of the sample implementation.
- Step 4: The compliance test procedures, tools, and sample implementation are used to validate the standard or change to the standard. Based on the review of the validation test results, a modification to the standard or proposed change, test criteria, test procedures, or sample implementation may be required. Follow-on testing should be conducted to validate the modification.

4.0 COMPLIANCE TEST AND EVALUATION

4.0.1 Compliance testing consists of a broad set of test objectives and should be tailored to a specific STANAG and the test environment. For example, a format standard may be tested by file exchange or by a rigorous test of the file production capabilities of a product or implementation. Other tests may only require physical measurements and/or verification of throughput or data flow.

4.0.2 Implementations that successfully complete compliance testing will be listed in a registry maintained by the Custodian for the applicable STANAG. This registry will include the name, version, and supported features of the implementation, the developer and sponsor, and the date of the test. Registration will normally be limited to a fixed term, such as two years, and actions will be required to extend the registration beyond that date. The requirement for registration expiration and the term of the expiration should be defined by the Custodian for the respective STANAG.

4.1 Compliance Testing

4.1.1 This testing is to verify that an implementation is compliant to a given standard. An implementation is initially tested for compliance against the standard. The standard defines which requirements are mandatory and which are optional. When performing the initial compliance test, all mandatory requirements, as well as optional features supported by the implementation, are tested.

4.1.2 If an implementation is changed in any way, retesting may be required. Retesting can be a complete test or can be a subset as mutually determined by the testing facility and the developer. Generally, retesting results in a new certification of the implementation.

4.1.3 Compliance certification can be based on a derived registration. A derived registration is one where a previous version of the implementation has been tested and the compliance has been successfully completed. An example would be if the registration has expired and the developer can demonstrate that neither the implementation nor the standard has changed. The certification of compliance can be renewed by derived registration. Another example is where an existing implementation is transferred to a new environment and the developer can show that the new environment (such as an update to an operating system) will not impact the proper operation of the implementation.

4.2 Reporting Changes Or Problems To Tested Implementations

4.2.1 Users of implementation who identify problems with certified implementations should report the problems directly to the developer. A courtesy copy of the report can be provided to the Custodian.

4.2.2 Developers and/or sponsors who have achieved certification of a given implementation must report hardware and/or software changes made to the implementation or problems identified with certified implementations. The report is made to both the testing facility that certified the implementation and the Custodian. As a result of the report, new testing maybe required.

4.3 Compliance Test Methodology

The process for verifying the compliance of an implementation against a STANAG is as follows:

- Step 1: The sponsor submits a request for compliance testing of an implementation to an accredited test facility.
- Step 2: The test facility and sponsor agree to the terms of the test, including the test criteria to be tested and the resources required (costs, personnel, schedules, location,

equipment, documentation, etc.).

- Step 3: The sponsor and/or developer submit the implementation to be tested and provide appropriate supporting documentation and resources to the test facility. The test facility conducts the test in accordance with the agreed criteria and procedures.
- Step 4: The test facility prepares a test report and provides a copy to the sponsor and developer. In cases where the implementation has deficiencies, the developer and test facility will coordinate the corrections and retest as necessary. The test facility provides a certificate of compliance to the developer and sponsor, and provides the registration information to the Custodian for incorporation into the registry, when testing is successfully completed.

4.4 Traceability of Test Results

When possible the results of compliance tests must be traceable to a recognized international reference standard. Where a STANAG requires implementation of a unique characteristic or capability for which no recognized international standard exists, test results must be traceable to a reference standard named in the Test Program Plan applicable to that STANAG.

4.5 Reporting Test Results

The form and format used to document compliance test results is to be agreed by the Test Sponsor and the Test Facility. However, test reports should include all information relevant to sample selection, test performance, and test results. As a minimum, information recorded for each compliance test must include:

- Identification of the system under test.
- Identification of the organization/agency conducting the test.
- Date the form was completed.
- Location of the system under observation.
- Data collector’s name , address and telephone number.
- Identity of the specific test performed.
- Identification of all test equipment used during the test.
- A diagram illustrating the interconnections between the system under observation and the test equipment used during the test.
- Test results.

5.0 INTEROPERABILITY TESTING/DEMONSTRATIONS

5.0.1 The purpose of interoperability testing and demonstration is to verify that certified implementations will interoperate in a joint or coalition environment. Compliance certification does not address the optional functionality present in many standards. These optional features may cause interoperability problems, which can only be identified through testing of multiple implementations together.

5.0.2 This test program will be conducted directly under the auspices of AG IV. The ISRIWG Chairman will identify a Demonstration Team leader and supporting demonstration team to oversee the interoperability testing and demonstrations. Some specific policies are applicable.

- Interoperability testing and demonstrations will be directly funded by the participants or through other resources.
- A demonstration plan will be prepared identifying the test objectives, procedures, and resources to be used. The plan will be presented to and approved by the ISRIWG and AG IV.
- Uncertified implementations should not be allowed to participate. Uncertified implementations add an additional level of uncertainty to the demonstration results. In addition, results of the interoperability tests can be iterated back into the certification program to improve certification testing.
- All interoperability testing and demonstrations should result in a final report to the ISRIWG and AG IV identifying successes and interoperability issues. This report will be prepared by the Demonstration Team and issues specific to a given STANAG will be provided to the Custodian for resolution.

6.0 TEST FACILITIES

6.1 General

Testing under this program will be performed at accredited test facilities. The accreditation process will be specified by the respective Custodian. The accreditation will be performed by the Custodian. Appeals of Custodian decisions can be made to AG IV. When more than one test facility is accredited for a specific STANAG, a lead test facility will be designated by the Custodian.

6.2 Accreditation

6.2.1 An AG IV member or any NATO organization may submit NIIA Testing Facility candidature to the Custodian. This candidature shall provide information in the following layout:

- Legal name of the test facility, full address, and contact information for authorized representatives, and identification of the authorized signatories.
- Declaration of the ownership of the facility.
- An organizational chart defining relationships relevant to the test services to be provided. Include a description of how they maintain an independent decisional relationship between themselves and their clients, affiliates, and other organizations.
- General description of test lab/facilities, scope of operations and NIIA-related test services, expertise/competence of personnel, and availability of appropriate test tools and procedures.

- A technical description of each type of testing supported (that is, a procedure describing the technical criteria tested and the way they are tested).
- Description of Test Procedures for certifying NIIA implementations.
- Description of procedures for scheduling test services and who can make use of such services.
- Information on how test services are funded.
- Statement of how the test facility will maintain knowledge, skill, and proficiency of its test personnel for the scope of NIIA related test services that they offer as well as an agreement to limit work/services to areas where competence and capacity are available.
- Statement on how they maintain records and that record of all service complaints and actions taken in response to complaints will be maintained.
- Declare that they will report to the accreditation authority (Custodian) within 30 days of any major changes involving location, ownership, management structure, authorized representatives, approved signatories, decreased expertise/competence, and/or the facilities of the laboratory.

6.2.2 The accreditation of the candidate will be determined based on its general capabilities and the completeness of its proposal. The Custodian will make the final determination and advise the test facility of the acceptance or rejection and reasons for rejection if applicable.

Acronym	
AEDP	Allied Engineering Documentation Publication
AG IV	Air Group IV (under CNAD/NAFAG)
ATTN	Attention
BE	Belgium
CNAD	Conference of National Armaments Directors
COTS	Commercial Off-The-Shelf
HQ	Headquarters
IEC	International Electrotechnical Commission
ISO	International Organization of Standardization
ISR	Intelligence, Surveillance, and Reconnaissance
ISRIWG	ISR Integration Working Group (under AG IV)
MNC	Major NATO Commands
NAFAG	NATO Air Force Armaments Group (under CNAD)
NATO	North Atlantic Treaty Organization
NIE	NATO Interoperability Environment
NIETWG	NATO Interoperability Environment Testing Working Group
NIIA	NATO ISR Interoperability Architecture
NIMP	NATO Interoperability Management Plan
POC	Point(s) of Contact
STANAG	Standardization Agreement
TBD	To Be Determined

Term	
Accreditation	The result of the process to establish an approved test facility for a given standard
Certification	The result of a successful compliance test – indicates that the implementation complies with the standard in question
Compliance test	A test conducted in a single implementation to show that the implementation complies with the provisions of the standard
Interoperability test	A test conducted on two or more implementations that show that when working together, the implementations can correctly function together
Validation test	A test conducted to show that a standard or change to a standard is accurate, complete, and understandable