NATO STANDARD

AEODP–03

INTER-SERVICE IMPROVISED EXPLOSIVE DEVICE DISPOSAL OPERATIONS ON MULTINATIONAL DEPLOYMENTS – A GUIDE FOR STAFF OFFICERS/OPERATORS

Edition D Version 1

FEBRUARY 2020

NORTH ATLANTIC TREATY ORGANIZATION
ALLIED EXPLOSIVE ORDNANCE DEVICE PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

28 February 2020

1. The enclosed Allied Explosive Ordnance Disposal Publication AEODP-03, Edition D, Version 1, INTER-SERVICE IMPROVISED EXPLOSIVE DEVICE DISPOSAL OPERATIONS ON MULTINATIONAL DEPLOYMENTS – A GUIDE FOR STAFF OFFICERS/OPERATORS, which has been approved by the nations in the MCLSB, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2370.

2. AEODP-03, Edition D, Version 1, is effective upon receipt and supersedes AEODP-03, Edition C, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database ((https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60

Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
DEU	According to Chapter 2, subsection 2.2, paragraph 2, destruction in situ may be carried out by non-trained personnel. DEU will deviate from this exception as according to national regulations Explosive Ordnances (EOs) including IEDs may only be disposed by appropriately trained personnel. According to DEU understanding, this also includes destruction in situ.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1 INTRODUCTION

1. Improvised Explosive Devices[1] (IEDs) can be a component of terrorism, criminality, disorder and insurgency[2]. They are an element of asymmetric warfare but exist across the spectrum of conflict and peacetime environments and are common in the Contemporary Operating Environment. IEDs create restrictions to movement and force protection, generate fear and uncertainty and have many other impacts; they hinder and may ultimately prevent the restoration of normality. They allow an enemy to both kill and harass and they serve to wear down our own forces, the other institutions of law and order and the general population.

2. IEDs can be simple or complex in their design. In some theatres the existence of Explosive Remnants of War can provide the IED builder with large quantities of explosive stores and the means to initiate them. Further components in the form of household electronics and telecommunications equipment are also readily available, and comparatively cheap. It is even possible that some hostile nations may engage their national scientific resources and explosives expertise in IED design and construction.

3. There are, by definition, no manufacturing standards for IED construction although trends may appear and there may be some commonality between IED components and between home-made explosives (HME). The safe conduct of IED Disposal (IEDD), therefore, principally relies upon appropriately trained and authorised IEDD Operators having a thorough knowledge of this area of expertise. This is underpinned by maximum situational awareness developed through continuous threat evolution analysis. Further details for IEDD Operator proficiency standards are contained within AEODP-10[3] (STANAG 2143). Details concerning Explosive Ordnance Disposal (EOD) roles, responsibilities and incident procedures are contained within AEODP-13[4] (STANAG 2377).

4. This document is subordinate to ATP-3.18.1[5] (STANAG 2282) and is intended as a guide both for staff officers and operators in the planning and conduct of IEDD operations. Every IED incident is unique and it is therefore not possible to lay down hard and fast rules, however guiding principles do apply. The principles outlined in this publication have been formulated as the result of lessons learned by many nations in theatres of operations around the world and can be applied to any IED situation.

[1] A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals, designed to destroy, incapacitate harass or distract. Note: It may incorporate military stores, but is normally devised from non-military components.
[2] For the purpose of this publication; terrorists, criminals and the proponents of disorder and insurgency will collectively be referred to as *enemy*.
[3] EOD Principles and Minimum Standards of Proficiency.
[4] EOD Roles, Responsibilities, Capabilities and Incident Procedures When Operating with Non EOD Trained Agencies and Personnel.
[5] Allied Tactical Publication for EOD.

1.2 AIM

1. The Aim of AEODP-03 is to highlight considerations and provide inter-service guidance for the planning and conduct of IEDD on multinational operations. All chapters are intended to be of relevance to EOD operators while EOD staff officers will find Chapters 1 and 2 most pertinent to the conduct of their duties.

1.3 SCOPE

1. This document is intended as guidance and a common framework as to the planning and conduct of IEDD operations, in conjunction with other NATO publications, documents and directives. It should be understandable to those who are unfamiliar with IEDD and EOD but is primarily aimed to inform and guide those who are trained in EOD/IEDD. It is designed to be applicable to all levels of capability but acknowledges that EOD Operators with different nations are not all trained, nor equipped, to the same level. Nations, and their individual armed services, have various capabilities as described in AEODP-13.

2. The document will focus on IEDD within deployed operations and will not explore IEDD within the framework of national home based/internal operations or military aid to the civil authorities, but can be used as a guide in these domains. The document is intended to provide guidance and considerations for the planning and conduct of IEDD operations and should serve to inform EOD Theatre Operating Procedures. IEDD is a sub-set of EOD and as such the detail of ATP-3.18.1 and associated EOD publications will apply and are not repeated here. IEDD is a component within the Defeat the Device pillar of the wider concept known as Counter-IED (C-IED)[6]. The doctrine for C-IED is contained in AJP 3.15[7] (STANAG 2295). As described in that publication, C-IED is a multi-agency function which seeks to identify and attack the whole IED system whereas IEDD concentrates on an individual event and the potential danger due to the device(s). Nevertheless, the choice of the EOD options to conduct IEDD will influence the quality of the exploitation which contributes to the other pillars.

3. IEDs may have additional payloads, including Chemical, Biological, Radiological or Nuclear (CBRN) and range from simple to complex. The threat from improvised CBRN devices, or toxic material in the vicinity of the device, must be considered when planning although the response will vary depending upon the operating environment, national capabilities and caveats. This document is not attempting to provide specific operating procedures and, as improvised CBRN devices will require a specialist response, they will not be covered in detail. The conduct of CBRN IEDD operations is detailed in AEODP-08[8] (STANAG 2609).

[6] The C-IED approach aims to defeat an adversary's IED System. The approach has 3 mutually supporting and complimentary pillars of activity which are: Attack the Networks, Defeat the Device, and Prepare the Force. These are all underpinned by understanding and intelligence.
[7] Allied Joint Publication for Countering Improvised Explosive Devices.
[8] Interservice CBRN EOD Operations on Multinational Deployments.

CHAPTER 2 PLANNING

2.1 CONTEXT AND ENVIRONMENT

1. The context and environment of the deployed operation should be considered when determining the IEDD response. The Combined Joint EOD (CJEOD) Cell will be responsible for conducting a threat analysis to determine the types of device and the modus operandi of the IED user. It is essential that this analysis be kept under constant review to establish trends and emerging threats and that it is included in the theatre specific Tactics, Techniques and Procedures (TTPs).

a. **Country Studies**. Country Studies prepared by Intelligence assets to identify geography, demographics, population details and history will assist in the preparation of background threat analysis. Additionally, these studies will help to determine such factors as key points, high value targets such as government institutions, economic or religious buildings, infrastructure or assemblies, MSRs, and other potential targets and/or vulnerabilities. Country Studies may be further enhanced by Intelligence Preparation of the Battlefield.

b. **Threat**. IEDD requires a thorough understanding of enemy intent, dispositions, modus operandi, configurations and capability including, equipment and logistics. Some information sought will be technical and IED focussed. A mixture of this intelligence is likely to be classified. Detail may be sourced from the Host Nation or other entities including security agencies, NGOs or International Organisations (IOs) such as the UN. Issues surrounding the sharing data between partner nations should be resolved at the earliest opportunity. Understanding the Threat is key in preparing the appropriate IEDD response.

c. **Operating Environment**. The operating environment and the threat to IEDD Operators will range between benign to hostile. It should be noted that this is irrespective of the type of conflict within the spectrum of war since *the Operator* may become a target. E.g. Peacekeeping may provide a hostile environment for IEDD Operators.

d. **Support of the Host Nation Population**. An environment whereby the Host Nation's population is compliant and supports IEDD activity (e.g. by obedience with instructions for cordons or willingness to provide information) will contrast with an environment where the population is hostile. Within a hostile environment flexibility of approach and force protection for IEDD Operators will become integral to delivering IEDD.

e. **Host Nation Security Services**. IEDD in peacetime is normally under the jurisdiction of the national police, fire department or security service and IED construction and placement are considered criminal or terrorist acts. Within deployed operations the status of Host Nation security services may vary between intact and capable to openly hostile. Nonetheless, they may retain primacy and/or a hybrid of responsibilities with NATO is possible. A large number of related considerations may therefore apply.

f. **Organizations**. IOs, NGOs and private actors can be involved in IEDD operations in a humanitarian framework such as during clearance of affected areas for restoration of economic normality. Their roles, responsibilities and the sharing of information with them must be considered with the aim of improving collective situational awareness.

g. **Legal Considerations**. In light of the above legal considerations are to be incorporated into IEDD procedures e.g. Issues of forensics, technical intelligence and evidence collection will apply in both the Host Nation and international arenas. Expert legal advice will certainly be required before formulating theatre/deployment specific procedures.

h. **Commanders' Intent**. Throughout the planning and execution of IEDD the commander's intent and his imperatives will apply. For example, force protection may be uppermost where the risk to Operators is to be minimised, alternatively the priority may be to maintain operational tempo where higher risks to Operators may be acceptable.

i. **Friendly Forces**. Knowledge of the IEDD capability and procedures of other nations and the agreed level of cooperation will be required in order to develop a balanced force package[9].

2.2 THEATRE PLANNING CONSIDERATIONS

1. **Configurations of IEDD Response**. Operational planners will need to determine (with EOD Subject Matter Expert (SME) advice) the optimum force structure for IEDD Teams in order to deliver the most effective IEDD capability for the operating environment. The IEDD response will be shaped by the threat, context and environment and the C-IED Approach. These considerations will balance, or perhaps compromise, agility with capability. The capability will be limited by the quantity of tasks it can deal with and the area over which they are spread. Such planning must be sufficiently flexible to permit agile adaptation of EOD force structures in response to evolution of the IED threat.

2. **Delivering IEDD**. IEDD should only be conducted by those who are suitably trained[10], equipped and authorized; national caveats will also apply as to what satisfies these criteria. Reporting, after action reviews and feedback mechanisms must be in place to ensure that risk controls are implemented and that the necessary adjustments are made on the TTPs, training and equipment of the IEDD capacities. Render Safe Procedures (RSPs) of IEDs are carried out by IEDD trained personnel, however, destruction in situ can also be carried out by non-trained personnel but the latter will be conducted at a greater risk with emergency means and acceptance of casualties by the tactical commander. This should be considered only in exceptional circumstances. The decision to do so should not normally be taken without an authorization process and mitigation measures such as in-Theatre training and the laying down of guidelines by the chain of command with EOD SME input. Furthermore, destruction in situ has a relatively low level of assurance and is likely to destroy exploitable material.

[9] Details of declared capabilities are referenced in AEODP-13.
[10] AEODP-10 deals with the *minimum* training standards for IEDD Operators.

3. **IEDD Support**. IEDD is a supporting activity e.g. delivering force protection or force manoeuvre. Nonetheless, IEDD will typically require additional support. There follows a list of considerations that are not intended to be comprehensive:

a. **Force Protection**. An IEDD Team is unlikely to be able to provide its own integral force protection.

b. **Scene Management**. An IEDD Team is likely to require support to manage an incident e.g. cordon troops.

c. **Electronic Counter Measures (ECM)**. Where there is a Radio Controlled (RC) or influence-fusing threat, ECM as a form of force protection is to be considered[11]. This specialised area is the provenance of Electronic Warfare (EW) specialists and specific regulations. Management of the electromagnetic spectrum will have many implications that are not listed here e.g. electromagnetic compatibility with other forms of communication. The responsibility for this lies with the Joint Force Communication Information Systems Cell and may be delegated to an EW Coordination Cell.

d. **Exploitation**. Incidents involving IEDs may provide technical intelligence and therefore should be investigated, where possible, by suitably trained staff and reported accordingly. EOD/IEDD contributes to technical exploitation of IED events though operators should be supported by specialists as necessary both in the tactical and forensic domains. Exploitation is undertaken to assist tactical, technical and forensic analysis. Exploitation of the device, its effects and tactics employed may assist with improving force protection, ECM, developing our TTPs, targeting IED networks, attribution of sources, and criminal investigation. Intelligence gained can subsequently be passed to assist C-IED possibly including other IEDD teams. Therefore, IED exploitation is a key part of the wider C-IED battle and should be afforded a high priority. Policies and procedures for exploitation are to be determined with J2 involvement.

e. **Medical Support**. In accordance with ATP-3.18.1, medical support arrangements should be considered.

4. **Post Incident Analysis**. Post Incident Analysis (PIA) should also be conducted to include reports from exploitation for the benefit of future C-IED activity e.g. to identify enemy trends, develop counter measures, and inform friendly tactics, training and procedures, information sharing and intelligence fusion. Provision for these activities must be incorporated into PIA. IED technical intelligence assessments are to be coordinated by appropriate HQ Staff[12] and disseminated down to the National Point of Contact for EOD (NPOCEOD) through Multinational EOD Coordination Cells (MNEODCCs).

[11] There may be requirements for EOD ECM over and above general force protection. ECM for EOD may have enhanced features.
[12] This should be accordance with theatre exploitation policy.

2.3 TECHNICAL CONSIDERATIONS

1. The conduct of an IEDD task and formulation of the RSP will be the responsibility of an IEDD Operator. In addition to the technical considerations, the RSP will also be influenced by the tactical situation and the operational imperatives. To assist planning staff, a number of basic considerations for an IED incident are outlined in the following paragraphs.

a. **Characterization and Categorization of IEDs**. As fully described at Annex A, IEDs may be characterized by their intended tactical employment and categorised by their technical description. Broadly, the 3 technical categories are: Time Operated, Command Operated and Victim Operated. Time Operated devices will normally attract the highest priority.

b. **IED Construction**. IEDs typically consist of 5 components: a switch, a power source, an initiator, a main charge and a container. Although the sophistication of the adversary and the availability of components will mean that devices encountered may differ, there are a number of common factors and methods of construction and operation that apply to almost all IEDs. Outward appearance is not always a reliable indicator but may signpost manufacture of IEDs in production runs to standard patterns. Therefore, as soon as a design has been established, full information on it should be published to all interested parties.

c. **Reducing an IED Hazard**. As with all EOD incidents, secondary hazards must be considered. The following means of reducing an IED hazard can be considered prior/to or in conjunction with an RSP.

(1) **Isolation**. Isolation of a device may assist in identifying secondary hazards.

(2) **Avoidance**. Avoidance may reduce the threat but may also allow the IED to be tampered with or otherwise may result in a loss of control of the device. This needs to be considered alongside returning to the device at a time of our choosing.

(3) **Removal**. Moving a device can be extremely dangerous. Remote means to do so should be considered.

(4) **Containment**. Containment for high explosives is difficult and can be time/labour/resource intensive.

d. **EOD Options**. The following EOD options for IEDD should be considered:

(1) **Destruction in Situ**. Destruction in Situ is a final disposal procedure (not an RSP) and risks an explosive event with attendant danger or damage to nearby life and property. It should only be employed where neutralisation carries a high risk to life or to the relevant operation.

(2) **Neutralisation**. This is an RSP. Neutralisation through remote disruption is the safest means and must be used whenever possible. Dismantling by hand carries a high risk and should only be used as a last resort.

(3) **Removal**. Moving a device may cause it to function and is only to be used where neutralisation and destruction in situ are impossible. Wherever possible, removal to a more accessible location should be accomplished by remote or semi-remote means, such as hook and line.

(4) **Containment**. If practicable and without detriment to the preservation of life or the operation, consideration should be given to the use of containment or protective works to reduce IED hazards.

e. **Technical Exploitation and Forensics**. Technical Exploitation and Forensics are a matter of expert assistance and may utilise a combination of in theatre, Host Nation or reach-back assistance. Teams may be configured with a selection of the following:

(1) Military / Civilian Police.

(2) IEDD Operators / Ammunition Technicians / Weapons Specialists.

(3) Scientists.

(4) Intelligence operatives.

(5) Other Specialists.

f. The work of technical intelligence, exploitation and forensics agencies (e.g. Weapons Intelligence Specialist, WIT, Combined Explosives Exploitation Centre) is vital to the C-IED and Counter Terrorism process. The interface between these and IEDD assets is critical and the appropriate protocols must be put in place at the planning stage and subsequently practised on deployment.

2.4 PROCEDURAL CONSIDERATIONS

1. **General**. All Operators must have an understanding of the authority under which they are acting. This must include who has primacy during an operation. In peace enforcement operations it is likely that, in the initial phase, primacy will be devolved to the deployed NATO force whereas in a benign scenario it is possible that the indigenous forces, either military or civilian, will retain primacy. It is also possible that as the operation proceeds primacy could change. Primacy issues must be included in the theatre-specific TTPs and it is essential that EOD personnel are kept informed of changes. It is a fundamental principle that a tactical commander cannot impose a RSP onto the IEDD operator.

2. **Suspect IED Reporting**. Responsible reporting of suspect IEDs is to be encouraged. Suspect objects/packages may look like an IED or suspicious acts may look like placement of an IED; these will remain as unconfirmed IEDs until further investigation has been carried out by an EOD Operator. The education of own troops and or the civilian population is an important

factor to consider. Of particular note is the need to use standard terminology at all levels to ensure the appropriate response and recording of information.[13] Other considerations such as tactical characterisation issues are dealt with elsewhere e.g. by the US IED Technical Exploitation Lexicon (TEL)[14]. These provide a framework of understanding and can be used as source documents for standardising the terminology and methodologies of related IED reports and returns. AEODP-06[15] (STANAG 2221) remains the authority on the content of IEDD reporting.

3. **Determining a Render Safe Procedure (RSP)**. The EOD Operator is responsible for determining the appropriate RSP for a given incident based upon an accurate threat assessment, and a combination of understanding Theatre TTPs, the tactical situation and the intent of the operational commander. However, it is not possible to dictate specific RSPs for every eventuality. There are, however, common safety factors that must be considered at every incident. In the event that the Operator requires advice relating to a proposed RSP or is unable to formulate an RSP, guidance should be detailed in TTPs and sought from the EOD authority equipped with appropriate technical oversight. This is often called 'referring up'.

4. **Categorisation and Prioritisation for IEDD**. IEDs are generally categorised according to their potential threat and are normally prioritised to determine how quickly action must be taken. Categories are assigned by the chain of command, based on EOD advice. However, in periods of intense IED activity, it may be left to the EOD Operator to assess the situation on his/her arrival at the scene and potentially change the incident category. Prioritisation is determined by operational imperatives. The criteria for assigning categories to EOD incidents are given in AEODP-10 as:

a. *Category A*. Assigned to EOD incidents that constitute a grave and immediate threat to life. Category A incidents are to be given priority over all other incidents, and disposal operations are to be started immediately regardless of personal risk.

b. *Category B*. Assigned to EOD incidents that constitute indirect threat. Before beginning EOD operations, a safe waiting period may be observed to reduce the hazard to EOD personnel.

c. *Category C*. Assigned to EOD incidents that constitute little threat. These incidents will normally be dealt with by EOD personnel after Category A and B incidents, as the situation permits, and with minimum hazard to personnel.

d. *Category D*. Assigned to EOD incidents that constitute no threat at present.

5. **Incident Control/IEDD Supervision**. Incident Control and IEDD supervision is based upon procedures detailed in AEODP-13. Additional factors such as ECM and forensic/technical intelligence gathering may need to be incorporated in TTPs. IEDD is conducted in accordance with EOD Safety Principles[16]. In addition the minimum size of an IEDD team is 2 appropriately qualified personnel.

[13] Technical EOD details are defined within the NATO TermDatabase.

[14] Though not a NATO document, the US IED Technical Exploitation Lexicon (5th Edn Dated 15 May 2017) can be obtained from the NSA MCLSB EOD WG website.

[15] EOD Reports and Messages.

[16] See ATP-3.18.1 Chapter 8, General Safety Principles and Specific Considerations.

6. **Evaluation/Threat Assessment**. During IED evaluation there will be many considerations that will remain theatre/situation specific and they are not listed here. MNEODCC should consider producing theatre checklists for IEDD evaluation/threat assessment and the subsequent IEDD plan. IEDD Operators are trained to conduct threat assessments and should assist in the theatre evaluation process.

7. **IEDD Philosophy and Principles**. IEDD procedures will be conducted by an EOD Operator who is appropriately trained and authorised. The need to avoid setting patterns is important to prevent Operators becoming targeted and IEDD procedures becoming predictable. In line with wider EOD doctrine[17], the IEDD **philosophy** is as follows:

a. Preservation of life.

b. Minimizing damage to health, property and the environment.

c. Preservation and collection of forensic material without unnecessarily compromising personal safety.

d. Restore freedom of movement as quickly as possible.

8. In addition there follows a list of guiding **principles** appropriate to the execution of IEDD:

a. **Remote Means** are to be used whenever possible within the tactical situation of the incident. Manual render safe action is only to be carried out as a last resort.

b. The Operator is to spend the **minimum amount of time** in the target area and is to return to the use of remote means whenever practicable.

c. **Soak periods** are periods of time where a manual approach is not made. The soak period is dependent on the types of delay mechanisms used in a given theatre and should be included in TTPs. Exceptions can be made to soak periods if operational priorities dictate or if through following the IEDD philosophy above is contravened.

9. **Mandatory Actions**. Mandatory Actions are designed to ensure IEDD operations are conducted in the safest possible manner and with appropriate technical oversight. They are to be determined and specified by the EOD chain of command in TTPs and must be observed. They are not aimed at restricting an Operator's choice of RSP and their application will be tempered by the operational situation.

10. **Examples of Mandatory Actions.** The following are examples for consideration that were commonly used and strictly adhered to in the past, it is accepted that they may not always be appropriate in a contemporary operating environment

[17] AJP 3.18 (STANAG 2628) – Allied Joint Doctrine for EOD Support to Operations.

a. Positive EOD action must not be conducted until appropriate cordon and evacuation measures are complete.

b. All manual approaches must be made as a one-man risk.

c. The EOD suit is to be worn on all manual approaches, except on Category A tasks or when it is likely to restrict the Operator.

d. Examples of mandated soak periods are described below:

(1) Primary Soak Period. The primary soak period is a minimum safe waiting period, derived from the current threat to be observed before a manual approach can be made to a suspect IED. The primary soak period should start from the time that the Operator is satisfied that the device has not been tampered with or otherwise changed.

(2) Secondary Soak Period. The secondary soak period is the minimum safe waiting time to be observed between positive EOD action and a subsequent manual approach. The time used should be a minimum time dictated by TTPs but is to be varied to avoid Operators setting patterns.

e. All suspect vehicles must be moved their own length, jolted and searched in detail before being handed over to other agencies agencies, except where they are observed being driven into position and immediately abandoned. This is to be done as part of the RSP, using remote or semi-remote means.

f. If the presence of an electronic or unrecognised timer is suspected, the Operator should, where practicable, refer up before a manual approach is made.

11. **Exemptions/Dispensing with Mandatory Actions**. The decision to dispense with a Mandatory Action is therefore only taken after consideration of all the known facts and operational imperatives. The Theatre EOD chain of command may preauthorise exemptions to mandatory actions and should consider the following:

a. **Primary Soak**. Before dispensing with a primary soak, consideration should be given to the vulnerability of Operators resulting from pattern setting. The mandatory primary soak period may be dispensed with in the following circumstances:

(1) **Tactical Situation**. There will be occasions when the tactical situation demands that the RSP for a suspect device must be undertaken immediately. In such situations, for instance when the cordon troops are under threat or the tactical commander needs to maintain the momentum of the operation, the Operator must decide whether normal procedures are appropriate or if alternative means, such as use of stand-off attack by armour or marking and avoiding might be more appropriate.

(2) **Category A Tasks**. At the scene of a Category A task, dependant upon the scenario, the Operator may dispense with the Primary Soak.

(3) **Explosions**. At the scene of an explosion the Primary Soak period may be dispensed with if the Operator can discount the possibility of additional devices.

(4) **Incendiary Devices**. Incendiary devices where no high explosives are involved.

(5) **Disruption**. Where disruptive action has taken place using remote techniques during the primary soak period and component separation is confirmed, and the Operator is satisfied that there are no other time initiated IEDs present then the primary soak can be dispensed with. However in order to prevent setting patterns the Operator should consider observing a secondary soak period.

(6) **Vehicle Clearances**. Primary soak may be dispensed with during vehicle clearances once the vehicles major load-carrying areas have been remotely cleared. This should include a thorough remote search inside and around the vehicle. However, if during any remote search, a suspect device is discovered and positive IEDD action cannot be taken, a Primary Soak is to be re-applied.

(7) **Suspicious Postal Items**. The Primary Soak period may be dispensed with once confirmation of postal transmission is established providing that the courier is not using predictable delivery times.

b. **Secondary Soak**. The secondary soak period may be dispensed with when the results of disruption are visible by remote means and component separation is positively established.

12. **EOD Suit**. The wearing of the EOD suit may be dispensed with for the preparation of equipment, but must be worn for the first positive IEDD action and subsequent manual approaches except in the following circumstances:

a. **Access/Tactical Situation**. When the Operator is faced with a difficult access problem or manual approach and the suit would only add to the danger present.

b. **Postal Devices**. Unless the courier is using predictable delivery times or if the item has been discovered as part of a find.

c. **Finds**. Finds that fall into one of the following categories:

(1) Occupied finds.
(2) Unoccupied finds where the possibility of anti-handling devices can be discounted.

d. **Accompanied by a Witness**. When it is necessary for the Operator to take a witness to be shown the location of a find.

INTENTIONALLY BLANK

CHAPTER 3 PROCEDURES

3.1 IEDD TASK PROCEDURES

1. **Establishment of an Incident Command Post (ICP)**. The Incident Command Post (ICP) [18] will normally be established by the Incident Commander (IC). *Note: For operations in support of civil authorities the term Incident Control Point may be used instead*.

2. **Recording of Team Routes and ICP Locations**. The EOD tasking authority should keep a record of task locations and routes used and the Operator should consult this record prior to deploying on a task and should plan a route accordingly in order to avoid setting patterns. In a non-permissive environment it may be important that IEDD Team routes to tasks and locations of ICPs may need to be varied, especially where there have been a number of tasks in the general area.

3. **Arrival at the ICP**. As soon as possible after arrival the Operator should be briefed by the IC as to the location and nature of the suspect item and also detail the actions taken to date on evacuating and cordoning the scene. It is at this point that the EOD Operator should determine the urgency of the tactical situation and be prepared to assist the IC, or local commander, in determining if the item should be the subject of a deliberate RSP or whether other means are appropriate e.g. other means might be the use of vehicle mounted guns or cannon, destruction in situ/blow in place or avoiding the area altogether.

4. **Establishing the EOD Control Point (ECP)**. The EOD Control Point (ECP)[19] must be established as soon as possible after arrival at the incident scene. The Operator should ensure that potential enemy firing points are dominated by friendly troops.

5. **Confirmation of ICP and ECP**. The ECP and ICP may need to be re-sited once the Operator has conducted a threat assessment. The possibility of deliberate entrapment, a *come-on*[20] situation, must be considered. If the proposed site has been used before, the Operator should consider alternate locations. In all cases the Operator must make sure that the locations are free of suspect devices and an appropriate 360 degree search should be undertaken.

3.2 INCIDENT MANAGEMENT

1. **Evacuation**. It is the IC, on the EOD Operator's advice, who must make the decision to evacuate a building or area when a suspect IED is found. However, the tactical situation will need to be considered. The following should be considered:

[18] Incident Command Post (ICP). The field location at which the primary tactical-level on-scene incident command functions are performed. It may be collocated with other incident response elements.

[19] EOD Control Point (ECP). The point through which the control of EOD activity is carried out by the EOD element. This may be situated with the ICP or elsewhere inside the cordon, depending on tactical requirements and EO hazards.

[20] Entrapment or *come–on* is a situation set by the enemy to deliberately encourage an IEDD team into the lethal area of an IED, often using a combination of 'concealed and deliberately overt devices.

a. Evacuation should never be past the IED.

b. Building exits near to the IED should be blocked and evacuation should be by alternative exits if practicable.

2. **Safety Distances**. Subject to the context/environment, the following distances are offered as a guideline for the initial evacuation and cordon:

a. Briefcase-sized device: 100m.

b. Car bomb: 200m.

c. Large IED (Includes van and truck bombs) or where secondary hazards are present: 400m.

3. **Considerations for Defeating Indirect Fire Weapons**. Indirect Fire weapons pose specific problems for the Operator. They can be wholly improvised or make use of improvised firing systems to project conventional ammunition items and they can be used in direct or indirect mode. In the case of a mortar, rocket or other stand-off weapon, the Operator must estimate the evacuation distances by considering the characteristics of the weapon system used.

a. With indirect fire weapons there are three areas to consider, these are:

(1) **Impact Area**. The impact area may contain blinds, partially functioned devices or explosion sites. Operators should be aware that there may be remaining unfired devices at the firing point or baseplate that could launch at any time.

(2) **Flight Path Area**. The range of improvised mortars can vary considerably and a corridor each side of the anticipated flight path should be considered to allow for possible airbursts or projectiles that drop-short.

(3) **Firing Point or Baseplate**. A large distance may have to be evacuated if it is suspected that:

i. There are unfired projectiles at the firing point or baseplate.
ii. The firing point or baseplate is in a vehicle.
iii. There is suspected self-destruct or anti-handling charge or secondary device at the firing point or baseplate.

b. The priorities for evacuation will normally be:

(1) Impact Area.

(2) Flight Path Area – including the corridor each side of the flight path.

(3) Firing Point or Baseplate.

c. However not all projectiles in an indirect fire system may have been activated and the priorities for Render Safe reflect this. The priorities for RSP are:

(1) Firing Point or Baseplate.

(2) Flight Path Area.

(3) Impact Area.

4. **Reducing Cordon Distances**. The Operator should ensure that potential firing points are dominated by friendly troops before endorsing a reduction in the cordon distance. Any such reduction is likely to be driven by the following considerations:

a. To minimise the possibility of the cordon troops coming under attack.

b. Where buildings act as a screen to reduce the effects of the IED.

3.3 SUPPORTING ACTIVITIES

1. **Witness Questioning**. After being briefed by the IC and prior to formulating a plan, the EOD Operator must gather information from all sources at the scene within the time constraints of the incident. He/she should question all witnesses who know anything about the circumstances surrounding the suspected IED and discard what is irrelevant. Witnesses available for questioning by the EOD Operator would normally be located at the ICP, preferably segregated from each other so that they cannot confer. A framework for the questioning that should be considered for IEDD tasks is at Annex B.

2. **IED Observation**. After questioning witnesses, the EOD Operator should, where possible, observe the IED and the surrounding area. He/she must consider doing this remotely; a manual approach should not be made simply to observe.

3. **Forensic Material Recovery**. The value of recovering forensic material will have to be balanced against the risk involved in collecting it. This is determined by the operational situation. Forensic material recovery is used for the following purposes:

a. **Force Protection**. Forensic material recoveries from IED attacks are used to inform and revise TTPs, assist in the development of ECM, improved armour and other force protection aspects. The value of forensic material recovery is increased when the device appears to differ from those previously encountered.

b. **Targeting**. Forensic recoveries are used to assist in identifying and targeting the enemy IED network.

c. **Attribution**. Items recovered from incidents and caches will be used to attribute IEDs to groups, nations or manufacturers for possible further action at the operational or strategic level.

d. **Prosecution**. Although impractical in many situations, items recovered in a forensically sound manner may be used in the prosecution of individuals

associated with the IED under host nation, national or international legal systems. In operations where the handling of criminal evidence is sub-optimal and the likelihood of court cases are diminished, forensic material recoveries can still have considerable value as a component of the international C-IED battle and should be collected whenever possible.

4. **IEDD Estimate and Plan**. The EOD Operator needs to make an accurate and logical assessment of the situation. This is best done by conducting an IEDD Estimate and Plan. Details of the IEDD Estimate and Plan are contained in Annex C.

3.4 EOD ACTION

1. **Implementing the RSP**. The EOD Operator must never become committed to following the plan slavishly but should remain flexible and keep his/her own safety uppermost in mind. When at the IED for the first time, the following points need to be considered against new factors and may cause the Operator to retire and re-plan:

a. Is the proposed RSP still feasible?

b. If the EOD Operator feels that he/she is spending too long at the IED, it indicates some weakness in the plan or in the implementation of the plan.

c. The EOD Operator should always keep asking himself/herself if any action is likely to move or disturb the IED.

d. Is the equipment being placed to give the best results?

e. Is any action being dictated by the fact that only certain pieces of equipment have been brought forward?

2. **Actions Following Positive Action (Remote or Manual)**. After each positive action, the EOD Operator must consider the following:

a. A remote approach is preferable.

b. Can the effects of the attack be seen? This may be achieved by deploying remote equipment with CCTV.

c. Is the next step in the planned RSP still practicable? If not, the Operator must re-plan before approaching.

d. What are the most appropriate tools to be taken forward on the next planned approach? The Operator should not make the approach empty handed or to simply observe.

e. When will it be safe to collect the remains for forensic evidence? The Operator must not cut into the IED without being sure that everything inside has been seen. It may be useful to use a hook and line to empty the contents of an IED

from its container or emply a through barrier detection system (e.g. x-ray) to determine contents.

3. **Continual Evaluation**. Continual re-evaluation must be ongoing throughout the task. As the Operator's actions continue, more information may come to light. Operators should use new information to modify their RSP if necessary.

4. **Confirming Clearance**. EOD teams are to confirm the clearance of found functional explosive devices or provide details of the remaining threat at an IED scene with regard to:

a. The Searching of suspect items.

b. Immediate area of a device.

c. Other areas may be searched at the Operator's discretion, based upon his threat assessment.

5. **Post RSP**. On completion of the RSP, the Operator is to:

a. Declare the task complete to the Incident Commander (IC).

b. Debrief supporting agencies where applicable.

c. Ensure that the cordon is maintained if forensic collection is required.

d. Assess and declare forensic material safe to handle and transport.

e. Inform the tasking authority of the task completion details.

6. **Documentation**. The Operator must complete an EO TASK REP[21] which is found in AEODP-06 (STANAG 2221). Additional reports may be required as ordered by SOPs.

[21] Explosive Ordnance Task Report.

INTENTIONALLY BLANK

ANNEX A IED CATEGORIES AND CONSTRUCTION

Information contained in this Annex is principally drawn from US IED Technical Exploitation Lexicon. Further detail can be extracted from that publication.

A.1. IED CHARACTERISATION AND CATEGORIZATION

1. Understanding of an IED incident requires consideration of two aspects:

   a. **Tactical Characterization**. The manner in which an IED incident is planned and conducted (tactical design) and the intent (purpose of device).

   b. **Technical Categorization**. A description of an IED using a hierarchical construct to identify its key components.

2. **Tactical Characterization**. This considers the Tactical Design of the IED along with the Purpose of Device.

   a. **Tactical Design**. The specific design of an IED attack – including but not limited to: position of the IED, the type of IED, type of road segment used, concealment technique, use of secondary devices, the time of day, etc. Tactical design addresses the questions: *Why here? Why now? Why in this way?*

   b. **Purpose of Device**. The immediate or direct tactical effect of the IED as summarised in Figure 1.

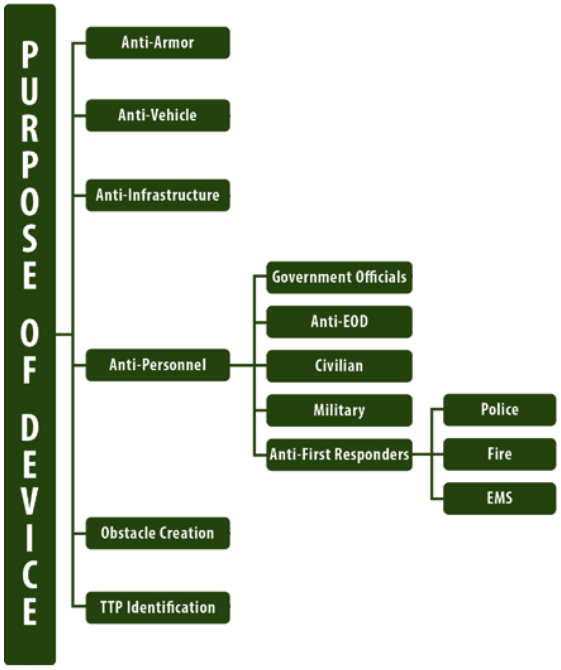

Figure 1. Purpose of Device.

3. **Technical Categorization**. As fully described at Paragraph A.2. and illustrated in Figure 2, a number of components are common to modern IEDs.

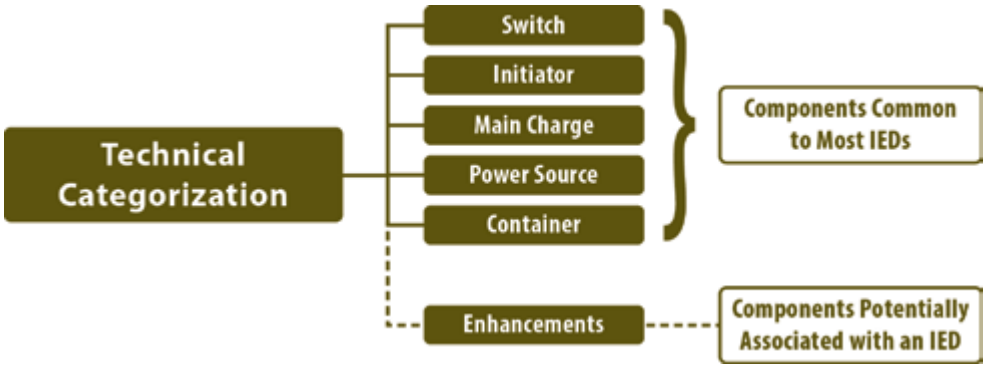

Figure 2. Technical Categorization.

A.2. IED CONSTRUCTION

1. **IED Components**. IEDs typically consist of the following 5 components (see Figure 3):

   a. A switch.

   b. A power source.

   c. An initiator.

   d. A main charge.

   e. A container.

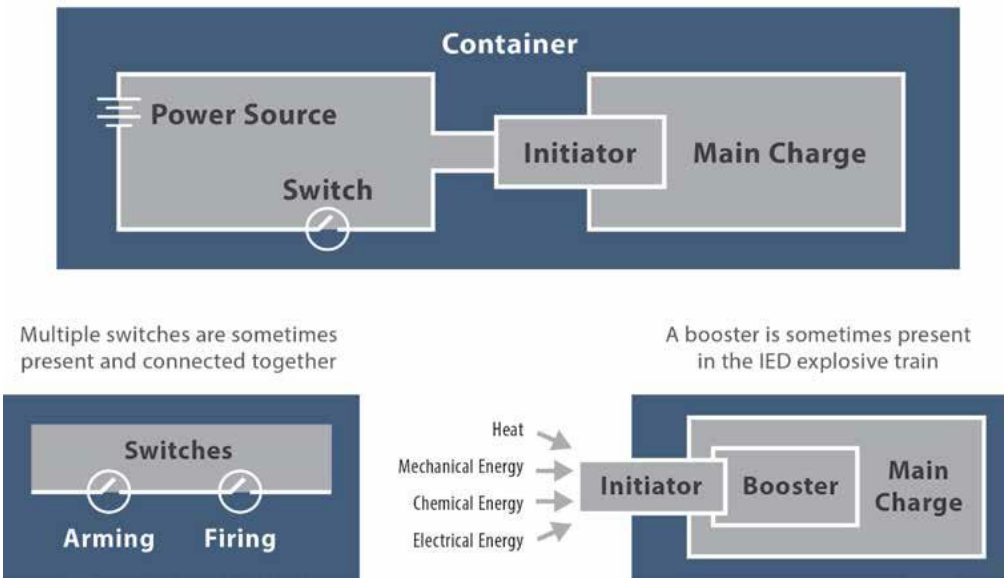

Figure 3. Components common to most modern IEDs.

2. **Switch**. As illustrated in Figure 4, there are 3 main types of switch, each of which have further subdivisions:

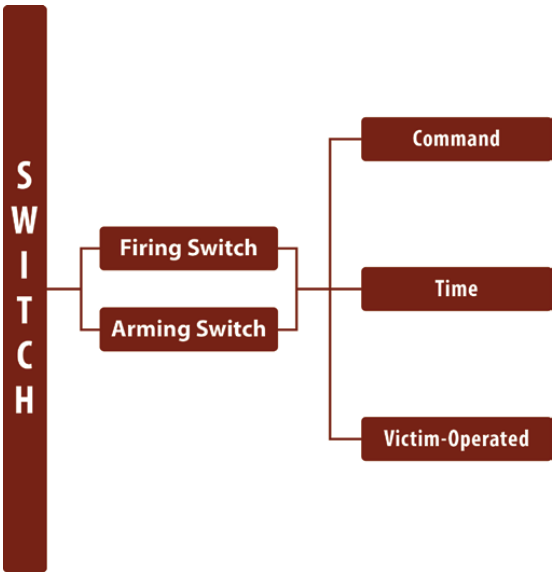

Figure 4. Types of Switch.

a. **Time Switch**. Time Operated IEDs are designed to function after a pre-determined delay. These are often used in anti-personnel (such as a secondary device to target the EOD Team or Cordon Troops), anti-property (such as a Large Vehicle-Borne IED (LVBIED)) or anti-forensic (such as an incendiary device in a vehicle that has launched an improvised mortar). There 3 types of time switch:

(1) Time Mechanical.

(2) Time Chemical.

(3) Time Electronic.

b. **Command Switch**. Command operated IEDs are designed to be initiated at the bomber's command, permitting him to choose the optimum moment of functioning. A physical link may exist between the firing point and the contact point or equipment incorporated which utilises the electromagnetic spectrum. Explosive elements of the IED may be set up as '*daisy chains*', whereby a number of explosive charges linked together with each charge being separated by up to 20 to 50m apart. There are 6 types of command switch:

(1) Command Wire.

(2) Pull.

(3) Radio Controlled.

(4) Command Light.

(5) Command Projectile.

(6) Command Acoustic

c. **Victim Operated**. Victim Operated IEDs are designed so that the victim causes the device to function. These are often used in devices such as: Under Vehicle IEDs, postal IEDs, pressure plate IEDs and Passive Infra Red (PIR) command armed victim operated devices. Light activated victim operated devices have also been used, particularly in dark spaces such as cellars. There are 8 types of victim operated switch:

(1) Pressure.

(2) Pressure Release.

(3) Pressure/Pressure Release.

(4) Sensor.

(5) Tension.

(6) Tension Release.

(7) Collapsing Circuit.

(8) Membrane Switch.

3. **Power Source**. All IEDs require a power source to provide the energy (electrical or mechanical) to initiate the device. The power source must be sufficiently durable to withstand the environment in which the device is stored or laid and must be commensurate with the desired size/weight of the IED. It must also be able to retain its power until the device is required to function. The main categories are:

a. **Electrical Energy**. Batteries or mains electricity.

b. **Mechanical Energy**. E.g. compressed spring.

4. **Initiators**. An IED can be initiated by various means including chemical, igniferous, percussion and electrical. For categorisation purposes these are described within 2 types of initiator, each of which has 3 further sub-divisions as shown in Figure 5:

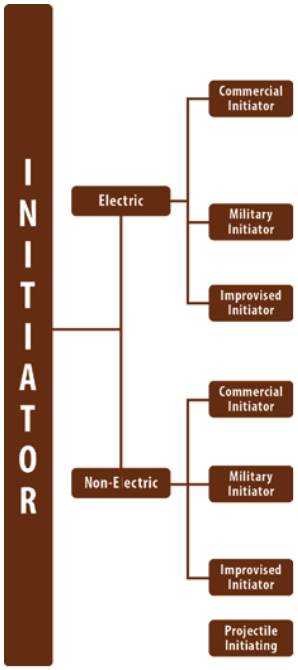

Figure 5. Types of Initiator.

a. **Electric**.

(1) **Commercial Initiator**. E.g. standard electric detonator, exploding bridge wire detonators or squibs/ignitors.

(2) **Military Initiator**. E.g. electric blasting cap or ignitor safety fuse electric.

(3) **Improvised Initiator**. E.g. flash bulb/light bulb plus HME.

b. **Non-electric**.

(1) **Commercial Initiator**. E.g. non-electric blasting cap or shock tube.

(2) **Military Initiator**. E.g. plain detonator or match fuse.

(3) **Improvised Initiator**. E.g. latex rubber plus acid.

5. **Main Charges**. The explosive charge which is provided to accomplish the end result in a munition. As shown in Figure 6, these can be categorised by explosive type (composition) and by the configuration of the main charge:

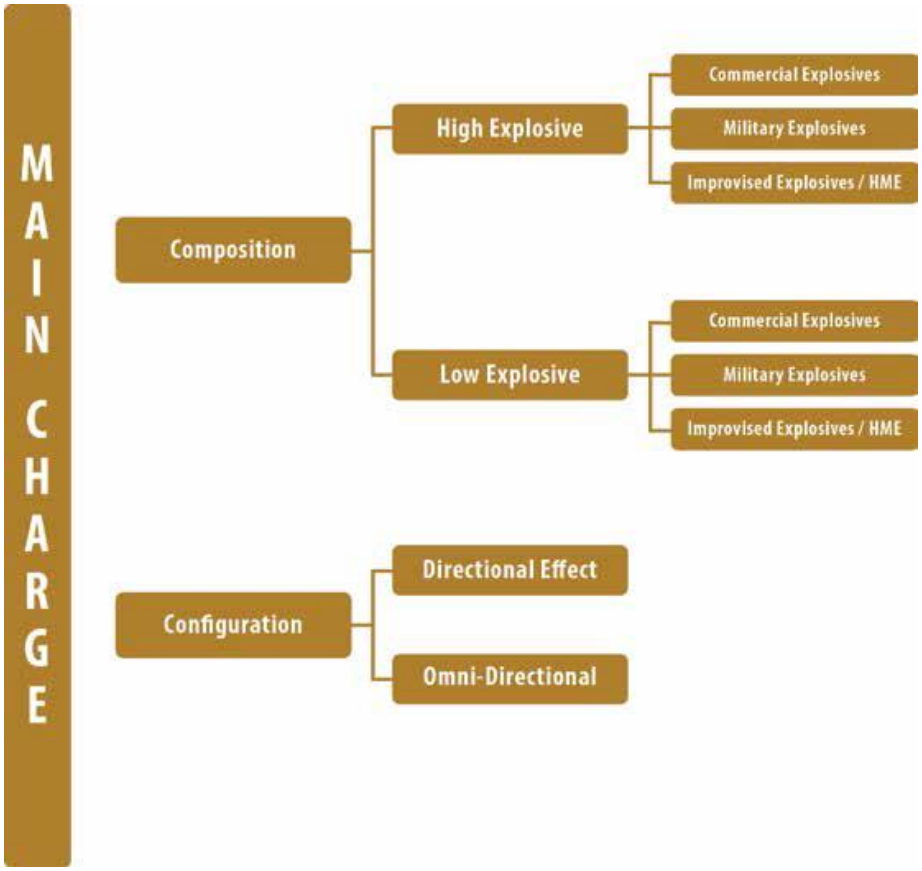

Figure 6. Main Charge Categorization.

a. **High Explosive**.

(1) **Commercial Explosives**. E.g. blasting agent, det cord or dynamite.

(2) **Military Explosives**. E.g. munitions or demolition materials.

(3) **Improvised Explosives/HME**. E.g. explosive compounds (such as TATP) or explosive mixtures (such as ANFO).

b. **Low Explosive**.

(1) **Commercial Explosives**. E.g. propellants or pyrotechnic fireworks.

(2) **Military Explosives**. E.g. propellants or incendiaries.

(3) **Improvised Explosives/HME**. E.g. explosive mixtures (such as HM black powder).

c. **Main Charge Configuration**.

(1) **Directional Effect**. E.g. improvised platter charge or improvised shape charge.

(2) **Omni-directional (blast effect)**. E.g. improvised grenade or mortar.

6. **Containers**. The container for an IED can come in virtually any shape or size varying from no container to one such as a briefcase, vehicle, drum, gas bottle, bottle or even a live or dead body. These can be subdivided as follows:

a. **Concealment**. A vessel commonly used to prevent the discovery of an IED by visual inspection. May also be used to add fragmentation.

b. **Confinement**. A vessel commonly used to hold the main charge together. May also be used to add fragmentation.

7. **Enhancements**. An optional, deliberately added component as opposed to a secondary hazard which modifies the effects of the IED. The IED would be effective, yet produce a different measurable result if this material were not added. The effect can be additional physical destruction, proliferation of dangerous substances (radiation, chemicals etc), or other results to enhance the effect of the IED Enhancements can be categorised as follows:

a. **Improvised**.

(1) Fuel.

(2) Fragmentation.

(3) Toxin (either animal, plant, human or synthetic).

(4) Chemical.

b. **Commercial/Toxic Industrial Materials**.

(1) Toxic industrial chemical.

(2) Toxic industrial biological.

(3) Toxic industrial radiological.

c. **Military/Weaponized**.

(1) Chemical agent.

(2) Biological agent.

INTENTIONALLY BLANK

ANNEX B IEDD WITNESS QUESTIONING

B.1. INTRODUCTION

1. An EOD Operator must develop a sound questioning technique for dealing with witnesses at the scene of a suspect IED. The following general tips on questioning technique should be borne in mind:

a. Witnesses should be interviewed separately, as people in stress situations tend to be confused and accounts of events can become contaminated by the accounts of others.

b. It is advisable to allow witnesses free rein to tell their story rather than interrupting with questions which may cause the witness to withhold information because the appropriate question was not asked. Only after their story has been told should the witness be questioned to fill in the gaps.

c. Questions do not always produce the answers required; the EOD Operator must ask himself *'What do I need to know?*' and then ask questions to gain this knowledge.

d. Each answer must be fully exploited. A useful technique is to ask of the answer received *'So What?'* or *'What does that mean to me in terms of my IED estimate?*

e. The EOD Operator should be firm and friendly and show no hostility towards witnesses. The Operator should remain impartial whilst listening but internally he should retain a degree of scepticism.

f. Where possible, other witnesses should be questioned to see if the facts can be corroborated.

g. It is useful to have a diagram drawn and have it confirmed in detail during the independent questioning of witnesses.

h. If a device functions during questioning witnesses, questioning should continue to try and establish whether other IEDs could have been placed. If the possibility exists then an appropriate soak period should be applied before investigating.

B.2. THE KEY QUESTIONS

1. Many questions may need to be asked to establish all relevant information. The key questions to be answered are often referred to as the '5 Ws':

a. *Where is it?*

b. *What is it?*

c. *When was it placed there?*

d. *Was anything seen or heard?*

e. *Why was it placed there?*

2. The questions are explained here in more detail:

a. ***Where Is It?*** This must be the first question asked to establish safety distances. The following key information should be obtained under this heading:

(1) A detailed description of the location of the device to enable the EOD Operator to use the remote equipment in the most effective way. Key considerations are the width of doorways and any steps or stairs. Even if a manual approach is resorted to, the precise location is required so that time spent in danger from the IED is reduced to a minimum.

(2) Whether anyone has been up to/come away from the IED and therefore whether a clear path has been established for the EOD Operator to use. A key question to anyone who has approached the IED is whether anything unusual was noticed on the path taken, such as wires, boxes, disturbed ground etc.

(3) Whether the suspect IED is placed on or near to any secondary hazard.

b. ***What Is It?*** Witnesses to the placing of the IED may be able to give an account of what was seen and heard, although it must be borne in mind that this information cannot always be totally relied upon. Descriptions of the size of the suspect IED will contribute to safety distance calculations and a *worst case option* should be considered.

c. ***When Was It Placed?*** This question has implications for the soak time on this information. If the accurate time of placement cannot be established, the EOD Operator must start the soak time from:

(1) The time that the security forces arrive on the scene and can guarantee that no one has tampered with the IED.

Or:

(2) The EOD Operator's time of arrival at the scene.

d. ***Was Anything Seen Or Heard?*** Witnesses' accounts of what the terrorist said or did can help the EOD Operator deduce the type of switching arrangement used in the IED. A description of who placed it may also be helpful.

3. ***Why Was It Placed?*** This is a question to himself. The answer to this question may give some indication of the source from which the IED came and therefore possibly the degree of sophistication or type of triggering system. The EOD Operator must be clear as to exactly what the target is as this in itself could point towards the likely method of operation of the IED. The EOD Operator should also consider whether the IEDD team or cordon troops may be the target.

INTENTIONALLY BLANK

ANNEX C IEDD ESTIMATE AND PLAN

C.1. INTRODUCTION

1. **The IEDD Estimate**. The EOD Operator needs to make an accurate and logical assessment of the situation. The estimate and plan for an IEDD task is broken into 4 parts. Although this may appear to be a time consuming process a well trained and experienced Operator should be able to accomplish the estimate quickly.

a. **Aim**. From arrival, the Operator must continually remind him/herself of the aim of the Operator's task.

b. **Factors**. Numerous factors will contribute to the development and continual re-evaluation of the RSP. As each factor is considered, the Operator must qualify it by asking the question '*So What?*' The main factors to be considered are:

(1) **Safety**. The size and location of the potential IED(s); the location of the ICP; cordon; evacuation; secondary hazards; assistance available from other agencies (e.g. gas/water/ electricity officials).

(2) **Enemy**. Enemy tactics, intentions, actions.

(3) **Target**. Who or what is the target and why?

(4) **Time**. Time device found and placed; warnings given; time available to the perpetrator; first and last light; time available for an RSP.

(5) **Intelligence**. Intelligence specific to the incident.

(6) **Suspect Device**. What, where, when, why, how found, size? Switch type? Secondary devices?

(7) **Ground**: Routes to and from the ICP for remote and manual approaches; use of ground by the enemy including line of sight, escape routes and the use of high ground.

2. **Courses Open**. The IEDD Operator is to consider:

a. **Insurgent/Criminal Courses of Action**. This is the Operator's assessment based upon the information obtained or available.

b. **Own Courses of Action**. From the Operator's deductions and assessment, options to be considered are:

(1) Immediate remote attack – time critical.

(2) Remote attack – not time critical.

(3) Semi-remote attack.

(4) Manual approach.

3. **Plan**. Once the most suitable course of action is decided, the Operator must formulate an outline plan that will become the basis for his/her RSP. The plan must be logically derived and consistent with the threat assessment. Concurrent activity must be maximised. Passage of information to the tasking cell must be considered and the plan must allow for:

a. The worst case effects of the IED functioning.

b. The failure of EOD action.

c. Any equipment problems that may occur.

C.2. EOD OPTIONS

1. The EOD options described at Paragraph 2.3 for IEDD should be considered:

a. Destruction in Situ.

b. Neutralisation.

c. Removal.

d. Containment.

2. **Remote Attack**. A consideration of the EOD Operator is whether he/she can deal with the IED remotely. The Operator must explore every remote method of attack. This entails mentally listing every weapon in the remote attack armoury and asking of each:

If I use it…..

What is the best that can happen?
What is the worst that can happen?
What is the most likely thing that can happen?

3. **Manual Approach**. Only after all plans of remote approach have been explored and discounted should a manual approach be considered. When planning a manual approach, the following factors apply:

a. The same questions for remote attack (shown above) should be explored for each of the possible manual approach methods. If the worst that can happen carries unacceptable risk, then another method that reduces that risk must be chosen.

b. The assessment can be helped by counting against each method how many manual approaches would be required. The Operator should also add the number of subsequent approaches that could be required if the primary

approach proves unsuccessful. The method which entails the least number of approaches is likely to be the safest.

c. Every possibility of reducing the amount of time spent in danger from the IED should be considered.

4. **Protection**. No protective measure can offer the EOD Operator absolute safety. He/she must guard against being lulled into a false sense of security and must take every measure to reduce risk wherever possible. Due consideration must be given to the following precautions which could give added protection to the EOD Operator:

a. The wearing of an EOD suit.

b. If the team vehicle is armoured it could be used to make part of the initial approach. It could be positioned at some midway point in order to reduce the length of time that the EOD Operator is directly exposed to the IED.

c. The cover from line of sight that buildings and other structures give must be exploited fully.

d. When there is a threat from local attack consideration should be given to the carriage of a personal weapon or the use of armed escorts at suitably safe distances and locations.

e. Active ECM should not be employed until the IC has confirmed that the cordon is established and evacuation has occurred. If active Electronic Counter Measures (ECM) is being employed, it must be remembered that they could cause the IED to function. Deconfliction of EOD ECM with force protection ECM is an essential part of planning.

5. **Discussion with the No 2**. After deciding the final RSP, the complete plan should be discussed with the No 2 in the EOD team. The old adage that ‘two heads are better than one’ is particularly relevant in an IEDD incident. It is important that the No 2 is encouraged to give his opinion.

6. **Briefing**. After discussing the task with the No 2, the No 1 must brief the EOD team members on the proposed RSP and their actions and responsibilities. The IC and other agency representatives must ideally be fully briefed on what their actions are to be at each stage and what the possible outcome of the RSP could be.

7. **Ongoing Communication**. The EOD Operator must ensure that communication is maintained with the IC throughout every phase of the task.

AEODP-03(D)(1)