UNITED STATES OF AMERICA	)	
	)	**Prosecution Objection to**
v.	)	**Providing an "Example" Witness**
	)	**to Examine the Viability of**
Manning, Bradley E.	)	**Reasonable Alternatives to Closure**
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	**Enclosure 2**
Joint Base Myer-Henderson Hall	)	
Fort Myer, Virginia 22211	)	**3 April 2013**

Encl 2 to
APPELLATE EXHIBIT 512
PAGE ___ OF ___ PAGES

Headquarters
United States Central Command
MacDill Air Force Base, Florida 33621

Regulation
Number 380-14

UNITED STATES CENTRAL COMMAND
SECURITY CLASSIFICATION GUIDE 0501

1. Purpose. This guide establishes the basic policies for proper classification, downgrading, and declassification of information related to the operations, facilities, communications, data collection and processing, warning, and other information pertaining to United States Central Command (USCENTCOM) and its components during normal periods and deployments for exercises and operations. This guide supercedes USCENTCOM Security Classification Guide 9901, dated 1 February 1999.

2. Applicability. This guide applies to the Headquarters, USCENTCOM; its components; and those government agencies, civilian contractors, and personnel involved in the activities of USCENTCOM.

3. Authority. The Original Classification Authority (OCA) for this guide is Lieutenant General Lance L. Smith, Deputy Commander, USCENTCOM. This classification guide reflects changes required by Executive Order (EO) 13292 dated 28 March 2003, "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information", and the Information Security Oversight Office (ISOO) Directive 1, 22 September 2003. Changes in classification markings are required in accordance with EO 12958, as amended. The classification authority for information covered under this guide shall be cited as shown below, along with the appropriate declassification instructions.

DERIVED FROM: USCENTCOM Security Classification
Guide 0501, Dated: 1 January 2005

4. Effective Date. This guide is effective upon receipt.

*This is a new regulation

5. Conflict/Changes. If this security classification guidance imposes impractical controls, or if changes are deemed appropriate, the U.S. government activity or civilian contractor organization concerned should forward recommendations and supporting rationale to the USCENTCOM SSO. Submission of such recommendations will not constitute authority to reclassify information and will not become an official change unless published as an update to this guide with the concurrence of the OPR.

6. Use and Reproduction of this Guide. This guide shall be used to determine the levels of the security classification to be assigned to information, systems, programs, plans, or projects associated with USCENTCOM. It may be necessary to consult separate classification guides to determine the degrees of security classification with respect to individual systems/subsystems, programs, plans, or projects that are USCENTCOM related. Reproduction of this guide is permissible.

7. Disclosure of Unclassified Information. DOD considers disclosure as the transfer of military information through approved channels to an authorized representative. When certain details of information are unclassified, it does not authorize automatic public disclosure. Proposed disclosure of unclassified information shall be processed through the Public Affairs Office (CCPA) and/or the Command Information Management Branch (CCJ6-PB), as appropriate. The term "disclosure" includes, but is not limited to, any technical data, articles, speeches, photographs, brochures, advertisements, presentations, and displays.

8. Disclosure of Classified Information.

a. To Other Government Agencies. Classified information regarding USCENTCOM may be disclosed to other DOD components, Federal agencies, or U.S. industrial facilities, only to properly cleared persons on a need-to-know basis in accordance with DOD 5200.1-R and USCENTCOM Regulation 380-1. It is the responsibility of the individual disclosing the information to verify the recipient's appropriate security clearance and need-to-know.

b. To Foreign Nationals. Classified information pertaining to USCENTCOM-related matters will not be disclosed to foreign nationals, foreign governments, or international organizations

without proper authorization per the National Disclosure Policy and USCENTCOM Regulation 380-5, upon coordination with CCJ2-FDO, the appropriate Director/Chief of Special Staff, and their designated Foreign Disclosure Representative.

c. Limitations. This guide should not be construed to allow the disclosure of proprietary information owned by private firms or citizens (i.e. patents, copyrights or trade secrets) to other contractors engaged in projects at USCENTCOM unless approved by the owner of such proprietary information.

9. Declassification and Downgrading. Information meeting the classification requirements of this guide shall remain classified as long as required by national security considerations. EO 12958, as amended provides uniform instructions for declassifying and downgrading national security information, including information relating to defense against transnational terrorism. These instructions are provided for each specific topic of information and they are not intended to be transcribed verbatim. They should be used to determine a specific date or event for declassification or downgrading. Specific declassification authority is not required to remark documents downgraded or declassified in accordance with instructions provided in this guide.

10. Organization of the Classification Guide (APPENDIX A).

a. Information Revealing. The "INFORMATION REVEALING" column states precisely the elements of information to be protected.

b. Classification. The "CLASS" column states which classification level applies to each element of information listed under the "INFORMATION REVEALING" column. The markings listed below are accompanied by descriptive extracts from DoD 5200.1-R:

(1) TOP SECRET. Applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe.

(2) SECRET. Applied to information, the unauthorized disclosure of which reasonably could be expected to cause

serious damage to the national security that the original classification authority is able to identify or describe.

(3) CONFIDENTIAL. Applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe.

(4) UNCLASSIFIED. Some UNCLASSIFIED information may be assigned FOR OFFICIAL USE ONLY (FOUO) status in the "REMARKS" column. FOUO is not a security classification, but a handling caveat. DOD 5400.7-R, DOD Freedom of Information Act Program, contains guidelines for properly marking, handling, and safeguarding FOUO information.

c. Declassification/Exemption. As of 22 September 2003, the use of X1, X2, X3, X4, X5, X6, X7, and X8 was no longer allowed as declassification markings. The "DECLASSIFY ON" column specifies the date or event for declassification or the 10-year automatic declassification exemption category as described in DOD 5200.1-R. If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision. When deciding how to complete the "Declassify on" line, an original classification authority will have the following choices:

(1) A date or event less than 10 years.

(2) A date 10 years from the date of the document.

(3) A date up to 25 years from the date of the document.

d. Reason. The "REASON" column specifies the reason for classification, citing the appropriate category of information listed in Section 1.4 of EO 13292, as follows:

(1) Military plans, weapons systems, or operations.

(2) Foreign government information.

(3) Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

(4) Foreign relations or foreign activities of the United States, including confidential sources.

(5) Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism.

(6) United States government programs for safeguarding nuclear materials or facilities.

(7) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism.

(8) Weapons of mass destruction.

e. Remarks. The "REMARKS" column contains any other pertinent information for each element of information, as appropriate, to include downgrading instruction, FOUO designations, etc.

11. PROPONENT. The proponent of this regulation is the Director of Intelligence, CCJ2. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQ USCENTCOM, ATTN: CCJ2-SSO, 7115 South Boundary Boulevard, MacDill AFB, FL 33621-5101, (813) 827-6281/6282 Fax: (813) 827-5484 (DSN: 651).

FOR THE COMMANDER:

JOHN G. CASTELLAW
Major General, USMC
Chief of Staff

OFFICIAL:

ANITA H. WRIGHT
LCDR, USN
Chief, Business Management
Branch

DISTRIBUTION:

C (1 EA), G

APPENDIX A
USCENTCOM Security Classification Guide 0501

MANPOWER, PERSONNEL, AND ADMINISTRATION (CCJ1)				
Information revealing	Classification	Declassification	Reason	Remarks
Country clearance requests	U	N/A	N/A	Will become classified if specific classified information is included (e.g., detailed travel itineraries of general/flag officers, etc.)
Daily personnel statistics	S	1 month	1.4(g)	Approximate numbers of deployed personnel may be released by the CCPA for official use

INTELLIGENCE AND SECURITY (CCJ2/JICCENT)				
Information revealing	Classification	Declassification	Reason	Remarks
Information concerning CI/HUMINT and other sensitive intelligence sources and methods	S	10 years	1.4(c)	May be classified higher if it incorporates information of a higher classification or by direction of the CCJ2 OCA
Intelligence information obtained from CI/HUMINT	C	10 years	1.4(c)	If the source is not identified
Intelligence exchange agreements	S	10 years	1.4(b) / 1.4(c)	
Products of analysis by USCENTCOM intelligence analysts	S	10 years	1.4(c)	May be classified higher if it incorporates information of a higher classification or by direction of the CCJ2 OCA

SECURITY (CCJ2-SSO)				
Information revealing	Classification	Declassification	Reason	Remarks
Approved modifications to the requirements of DOD 5200.1-R during operations	C	Upon completion of operation	1.4(g)	
Damage assessments conducted pursuant to the loss or compromise of classified information	C	10 years	1.4(g)	May be classified higher based on content
Exploitable information or personnel security weaknesses in OCONUS areas	C	Upon correction, elimination of weakness, or 10 years, whichever is sooner	1.4(g)	
General security countermeasures	U	N/A	N/A	
Loss of classified material	C	Upon regaining custody of material or following completion of damage assessment, whichever is later	1.4(g)	
Weaknesses in the application of security measures for safeguarding classified information during operations, in OCONUS locations, or during periods of increased threat	C	Upon correction of weakness or completion of the operation, whichever is sooner	1.4(g)	

SYSTEMS (CCJ2-S)				
Information revealing	Classification	Declassification	Reason	Remarks
ALE password	TS	Upon change	1.4(a)	SCI
COLISEUM password	TS	Upon change	1.4(a)	SCI
DAWN/HOCNET password	S	Upon change	1.4(a)	
GALE password	TS	Upon change	1.4(a)	SCI
JWICS LAN/WAN user ID	U	N/A	N/A	
JWICS LAN/WAN password	TS	Upon change	1.4(a)	SCI
RMS password	TS	Upon change	1.4(a)	SCI
SAFE password	TS	Upon change	1.4(a)	SCI
Virus/network intrusions	S	Once neutralized	1.4(g)	
XDITDS password	TS	Upon change	1.4(a)	SCI

OPERATIONS (CCJ3)				
Information revealing	Classification	Declassification	Reason	Remarks
Exercises (CCJ3-E)				Separate classification guidance shall be issued by CCJ3-E for exercises. CCJ3-E will issue a by-country yearly guide or a guide for each specific exercise. For further information, contact CCJ3-E

STRATEGIC DEPLOYMENT (CCJ3-S)				
Information revealing	Classification	Declassification	Reason	Remarks
C-Date/calendar date association	C	3 years after completion	1.4(a)	
Concept of operations	S	1 year after completion	1.4(a)	Confidential upon execution
Exercise name	U	N/A	N/A	
Exercise/operation location	S	Upon execution	1.4(a)	If classification/ declassification instructions are not specified by JCS/HN
Exercise/operation name associated with host nation (HN)	S	Upon execution	1.4(a) / 1.4(d)	If classification/ declassification instructions are not specified by JCS/HN
Exercise/operation name associated with participating units	S	Upon execution	1.4(a)	If classification/ declassification instructions are not specified by JCS/HN
Operation code words	S	1 year after completion	1.4(a)	Confidential upon execution
Participation of a specific individual in operation	U	N/A	N/A	
Participating units, including types, vulnerabilities, locations, quantities, readiness status, deployments, redeployments, and details of movement of U.S. and friendly forces in operation	S	Upon execution or following release by national command authorities, whichever is sooner	1.4(a)	If classification/ declassification instructions are not specified by JCS/HN
Information revealing	Classification	Declassification	Reason	Remarks
Units/HN association	S	1 year after completion	1.4(a) / 1.4(d)	Confidential upon execution

LOGISTICS AND ENGINEERING (CCJ4/7)				
Information Revealing	Classification	Declassification	Reason	Remarks
Analysis and impact of all USCENTCOM AORs	C	Upon completion of mission	1.4(d) / 1.4(g)	Negotiations of construction projects, AIK, customs issues, etc
Bilateral OPLAN execution logistics and support requirements with AOR partners	C	10 years or upon completion of project, whichever is sooner	1.4(a) / 1.4(d)	
Characteristics of U.S. weapons and related sustainability	S	10 years	1.4(a)	May be classified higher upon direction of an OCA
Deployment/redeployment of units	C	Upon completion of mission or following release by national command authorities, whichever is sooner	1.4(a) / 1.4(g)	May be classified higher upon direction of the CCJ4/7 OCA
Force protection threat analysis	S	Upon completion of mission	1.4(g)	Includes intelligence efforts and threat weapons
Identification of forward headquarters	S	10 years	1.4(a) / 1.4(g)	Purpose of facility is classified. Description as school house" is unclassified.

LOGISTICS AND ENGINEERING (CCJ4/7) Cont.				
Information Revealing	Classification	Declassification	Reason	Remarks
JA1 fuel inventory	S	10 years or upon completion of mission, whichever is sooner	1.4(g)	Classified when inventory is related to days of war supply
MOBSTR-B	S	Upon completion of mission	1.4(g)	Location/ capabilities of relay system for U2
Movement of ammunition, aircraft, personnel, units, or communications equipment	C	Upon completion of mission	1.4(a) / 1.4(g)	May be classified higher upon direction of an OCA
Movement of sensitive or critical supplies/personnel	C	Upon completion of mission	1.4(a) / 1.4(g)	May be classified higher upon direction of the CCJ4/7 OCA
Number of aircraft in AOR	S	Upon completion of mission	1.4(g)	Coalition aircraft report (If classification/ declassification instructions are not specified by JCS/HN)
Proposed U.S. positions or strategy of negotiations	C	Upon completion of mission	1.4(a) / 1.4(d)	Negotiations of construction projects, assistance in kind (AIK), customs issues, etc.
War reserve stockage data	S	10 years	1.4(a) / 1.4(g)	

PLANS AND POLICY (CCJ5)				
Information Revealing	Classification	Declassification	Reason	Remarks
Beddown sites	S	10 years or upon plan execution, if executed	1.4(a)	
Capabilities-based munitions requirements	S	10 years	1.4(a)	
Chemical/biological weapons and proliferation plans	S	10 years	1.4(a) / 1.4(h)	
Command and control relationships	U	N/A	N/A	
Commander's intent	S	10 years	1.4(a)	Confidential upon plan execution
Deception plans for operations	TS	10 years	1.4(a)	
Defended assets list (DAL)	S	10 years	1.4(a)	
Essential elements of friendly information (EEFI)	S	10 years	1.4(a)	Complete detailed list
Force lists	S	10 years	1.4(a)	Confidential upon plan execution
HN participation	S	10 years or upon plan execution, if executed	1.4(a) / 1.4(b)	
Joint monthly readiness review (JMRR)	S	10 years	1.4(a)	

PLANS AND POLICY (CCJ5) Cont.				
Information Revealing	Classification	Declassification	Reason	Remarks
Location and designation of USCENTCOM representatives	U	N/A	N/A	
Mission statements	S	10 years	1.4(a)	Confidential upon plan execution
NBC operations	S	10 years	1.4(a)/1.4(h)	
Plan briefs	S	10 years	1.4(a)	
Plan phasing	S	10 years	1.4(a)	
Planning directives	S	10 years	1.4(a)	Confidential upon plan execution
Planning milestones, internal suspense dates	U	N/A	N/A	
Rules of engagement	S	10 years or upon plan execution, if executed	1.4(a)	
Strategic concepts	S	10 years	1.4(a)	
TPFDD plan identifiers, except:	U	N/A	1.4(a)	
- Aggregate tonnage/pax	U	N/A	N/A	
- U.S. unit name and destination com ined (except SOF)	U	N/A	N/A	
- U.S. unit name with EAD/LAD	U	N/A	N/A	
- U.S. unit name with UIC/ULN	U	N/A	N/A	

PLANS AND POLICY (CCJ5) Cont.				
Information Revealing	Classification	Declassification	Reason	Remarks
- ULN and destination	U	N/A	N/A	
- ULN and EAD/LAD	U	N/A	N/A	
- Origin, UIC, and ULN	U	N/A	N/A	
- Flight plans for logistics support	U	N/A	N/A	
War plan short title combined with long title	S	10 years	1.4(a)	
War plan short title or long title standing alone	U	N/A	N/A	

DELIBERATE WAR PLANS (CCJ5-P)				
Information revealing	Classification	Declassification	Reason	Remarks
Characteristics of U.S. weapons and related sustainability	S	10 years	1.4(a)	May be classified higher upon direction of an OCA
Communications effectiveness, sustainability, limitations	S	10 years	1.4(a)	
Concept of operations including order of battle, execution circumstances, operating locations, resources required, tactical maneuvers, deployments, actions and objectives	S	10 years	1.4(a)	Confidential upon plan execution
DEFCON meaning and status	S	10 years	1.4(a)	
Synchronization matrices	S	10 years	1.4(a)	
Plan(s) timelines	S	10 years	1.4(a)	
Flexible deterrent options	S	10 years	1.4(a)	
Estimates of operational effectiveness of intelligence, counterintelligence, rescue, and reconnaissance	S	10 years	1.4(a)	

DELIBERATE WAR PLANS (CCJ5-P) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Limitations and vulnerabilities of U.S. forces in the combat area	S	10 years	1.4(g)	
Location, itineraries, and travel modes of key U.S. and friendly military and civilian leaders	S	10 years	1.4(a)	Confidential upon execution of VIP travel
Nuclear weapons; potential use of	S	10 years	1.4(a) / 1.4(h)	
Operation code words	S	10 years	1.4(a)	
Participating units, including types, vulnerabilities, locations, quantities, readiness status, deployments, redeployments, and details of movement of U.S. friendly forces	S	10 years	1.4(a)	Confidential upon plan execution
Plan classification guide	C	10 years or upon plan execution, if executed	1.4(a)	
Planning assumptions	S	10 years or upon plan execution, if executed	1.4(a)	

DELIBERATE WAR PLANS (CCJ5-P) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Status and details of U.S. alliances, including status of forces, deployment rights, privileges, airfield use, and port availability	S	10 years	1.4(a) / 1.4(d)	
Friendly centers of gravity	S	10 years	1.4(a)	
War termination objectives	S	10 years	1.4(a)	
End state of plan	S	10 years	1.4(a)	
Target area weather information	S	10 years or upon plan execution, if executed	1.4(a)	
Top secret options; discussion of	TS	10 years	1.4(a)	
Limitations and vulnerabilities of U.S.	S	10 years	1.4(g)	

COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6)				
Information revealing	Classification	Declassification	Reason	Remarks
Communications networks, users, frequencies, call signs, HJ times, and identification of net control stations	S	When superceded	1.4(a) / 1.4(g)	
COMSEC incidents/violations	C	10 years	1.4(g)	
Composite list of COMSEC short titles	C	10 years	1.4(c)	
Cryptology	S	10 years	1.4(c)	
Communication outages that degrade command and control capability	S	Upon restoration of capability	1.4(g)	
Scheduled down times of communications systems	S	10 years	1.4(g)	
GCCS User ID	U	N/A	N/A	
GCCS Password	S	When changed	1.4(a)	
Specific locations of deployed communications units	S	Upon redeployment	1.4(a) / 1.4(g)	
Specific locations or countries planned for employment of elements of Defense Communications Systems - Central Area (DCS-CA)	S	10 years	1.4(d)	

COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Specific locations or countries in which DCS-CA are employed	S	10 years	1.4(d)	
Details revealing specific units supported by DCS-CA	S	10 years	1.4(c) / 1.4(g)	
Details revealing force locations, by type, for war plan employment of DCS-CA	S	10 years	1.4(a)	
Specific locations or countries in the AOR in which communication equipment is identified as supporting the DCS-CA	S	10 years	1.4(d)	
Identification of an operational shortfall or limitation In war-fighting capabilities of DCS-CA	S	Upon correction	1.4(g)	
Details of the capability required to achieve the initial operational capability of DCS-CA	S	Upon full operational capability	1.4(g)	

COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
A description of the DCS-CA system and details of the capability required to achieve full operational capability	U	N/A	N/A	
A description of the composition of a DCS-CA node at full operational capability	U	N/A	N/A	
Characteristics of the DCS-CA	U	N/A	N/A	
Cost/Budget data on the DCS-CA	U	N/A	N/A	
Identification of the agencies responsible for the various aspects of system acquisition, implementation, operation, and maintenance	U	N/A	N/A	
Required capability dates, initial operational capability, and full operational capability dates	U	N/A	N/A	
Frequencies lists	U	N/A	N/A	
Contingency and Operational Joint Communications Electronics Operating Instructions (JCEOI)	S	When superceded	1.4(a)	Unclassified for training within the U.S. Releasable to MNF when part of Coalition

COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6) Cont.				
Information revealing	Classification	Declassification	Reason	Remarks
Frequency lists used in the AOR associated with the location/coordinates, date/times of use, operating units, and detailed purpose of the frequency (Example: Force Protection Net)	S	When superseded	1.4(a)	List of frequencies alone are Unclassified
Frequency lists used in the AOR required for coordination with the host nation may only be associated with the location/coordinates, date/times of use of the frequency (Example: Land Mobile Radio Communications)	U	N/A	N/A	Information required to be released is considered FOUO (DOD 5400.7-R)
Joint Restricted Frequency Listings (JRFL)	S	When superceded	1.4(a) / 1.4(c)	Releasable to MNF when part of the Coalition. Determined by Command Electronic Warfare Officer (EWO)

RESOURCES AND ASSESSEMENT (CCJ8-AR)				
Information revealing	Classification	Declassification	Reason	Remarks
Products of analysis by USCENTCOM operations research analysts	S	10 years	1.4(a)	May be classified higher if it incorporates information of a higher classification or upon direction of an OCA
Requirements documents identifying USCENTCOM future operational needs in support of CDR USCENTCOM strategy	S	10 years	1.4(a) / 1.4 (b) / 1.4 (e) / 1.4 (g)	

SCIENTIFIC ADVISOR (CCJ8-TI)				
Information revealing	Classification	Declassification	Reason	Remarks
Vulnerabilities of new military technologies	S	10 years or upon correction, if corrected	1.4(e) / 1.4(g)	
New operational concepts based on application of new technologies	S	25 years	1.4(e)	
Requirements documents identifying critical military deficiencies	S	10 years	1.4(g)	

COMMAND GROUP (CCCC)				
Information revealing	Classification	Declassification	Reason	Remarks
Detailed travel itinerary of USCENTCOM Commander	S	Upon completion of travel	1.4(a) / 1.4(g)	Classified when information reveals name/title associated with dates/times or locations
Detailed travel itineraries of General/Flag officers and civilian equivalent	C	Upon completion of travel	1.4(a) / 1.4(g)	Classified when information reveals name/title associated with dates/times or locations

Attack the Network – Defeat the Device – Train the Force

SECURITY CLASSIFICATION GUIDE

for

JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT ORGANIZATION (JIEDDO)

DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD contractors only, administrative or operational use, effective the approval date of this document. Other requests for this document shall be referred to the JIEDDO Security Office.

This document contains information EXEMPT FROM MANDATORY DISCLOSURE Under the Freedom Of Information Act (FOIA). Exemption 2 applies.

APPELLATE EXHIBIT 512, ENCL 2
PAGE REFERENCED:____
PAGE____OF____PAGES

Security Classification Guide

for

Joint Improvised Explosive Device Defeat Organization (JIEDDO)

Date: _____

Approved By: _____
Michael D. Barbero, LTG
Director
Joint IED Defeat Organization

Issued By: Joint IED Defeat Organization
5000 Army Pentagon
Washington, DC 20310-5000

Action Officer: Mr. John E. Nimitz
Security Officer/SSR
Joint IED Defeat Organization
703-601-4744

1. PURPOSE

This Security Classification Guide (SCG) is a living document that provides guidance and instructions on the classification, marking and distribution of information involved in the development and eventual employment of tactics, techniques, procedures (TTP) and technologies that enable the Joint Improvised Explosive Device Defeat (IED) Organization (JIEDDO) to defeat the IED threat. This SCG addresses security measures to safeguard developmental efforts within the organization as well as already developed end items that require ongoing protection measures. As the organization matures, JIEDDO will update the SCG to address additional IED defeat developmental efforts requiring protection. Future revisions to this SCG will update declassification dates in light of fielding dates and other program milestones, as well as technology commercialization and/or obsolescence. Any suggested changes or updates to this SCG will be provided in writing to the Office of Primary Responsibility (OPR) as indicated in paragraph three.

2. AUTHORITY

This SCG is issued under authority of Executive Order (E.O.) 12958, as amended 25 March 2003, and DoDI 5200.1-R (Information Security Program). This SCG constitutes authority and may be cited as the basis for classification, downgrading, or declassification of material related to the JIEDDO activities in support of DoD Directive 2000.19E, Joint Improvised Explosive Device Defeat. Unless otherwise noted, information or material identified as CLASSIFIED by this SCG is classified by authority of the JIEDDO Original Classification Authority identified on the title page.

3. OFFICE OF PRIMARY RESPONSIBILITY (OPR)

This SCG is issued by and all inquiries for information concerning its content should be addressed to the Joint Improvised Explosive Device Defeat Organization (JIEDDO), Attn: Director, 5000 Army Pentagon, Washington DC 20310-5000.

4. CLASSIFICATION CHALLENGES

Questions concerning the content and interpretation of this SCG should be directed to the issuing activity. If the security classification imposed by this SCG is considered impractical, documented and justified recommendations should be made through appropriate channels to the issuing activity. If current conditions, progress made in this effort, scientific or technological developments, advances in the state-of-the-art or other factors indicate a need for changes, similar recommendations should be made. Pending a final decision, the information involved will be protected at either the currently specified level or the recommended level, whichever is higher. All users of this SCG are encouraged to assist in improving its currency and adequacy. Any classification challenges should be brought to the attention of the OPR.

5. REPRODUCTION, EXTRACTION AND DISSEMINATION

Copies of this SCG and all extracts thereof will be made, stored, and transmitted in accordance with (IAW) authorized procedures corresponding to the classification of the information involved. Authorized recipients of this SCG may reproduce, extract, and disseminate the contents of this SCG, as necessary, for use by specified groups, including industrial activities that are involved in IED Defeat development, test, or operations.

6. PUBLIC RELEASE

The fact that this SCG contains certain details of unclassified information does not permit automatic public release of the information. Proposed public disclosures of the JIEDDO's unclassified information regarding the technologies and activities shall be processed through appropriate channels for approval to publish. Requests for public release certification must be submitted in accordance with DoD Directive 5230.9 (Clearance of DoD Information for Public Release), DoD Regulation 5400.7 (DoD Freedom of Information Act Program), and the Industrial Security Manual for Safeguarding Classified Information (Section 5 Disclosure). Defense contractors, military members as well as government service employees shall comply with DoD Manual 5220.22-M (National Industrial Security Program Operational Manual (NISPOM)) and other requirements that may be directed by the Government.

Only information that has been reviewed and certified for public release may be released. However, the decision or authority to release information belongs to the Public Affairs office. The OPR will process requests for approval as outlined below.

Any proposed release to the public of official information pertaining to the JIEDDO must be forwarded to the JIEDDO, STRATCOM for review and further processing. The term "release" applies, but is not limited to, articles, speeches, briefs, papers, photographs, brochures, advertisements, displays, presentations, etc., on any JIEDDO related activity. It is incumbent upon defense contractors, or other agencies, to screen all information submitted by them for the material certification to ensure that it is both unclassified and technically accurate. Letters of transmittal shall contain certification to this effect. The number of copies produced, and distribution of the document, must be strictly controlled until review is completed. If suspected classified information is found during the review process, all holders of the document will be informed of the degree of protection required. When doubt exists concerning the classified status of a proposed release pertaining to the JIEDDO, Security will render the final decision. The material submitted for review must include a valid suspense date, if applicable. Requests for public release certification, according to DoD Manual 5220.22-M, NISPOM (attachment to DD Form 441, Security Agreement), must be submitted to the JIEDDO, STRATCOM for review and further processing. Electronic copies (unless submitted via Secret Internet Protocol Router Network (SIPRNet)) of the proposed public release material must be submitted to JIEDDO, STRATCOM at least two weeks before approval is needed.

Approval for public release does not necessarily satisfy export-licensing requirements of the Departments of State and Commerce. Export-controlled material will not be entered into the security review channels for public release approval to circumvent the licensing requirements of the Departments of State and Commerce.

Release of Program Data on the World Wide Web: Extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. The search and data mining capabilities of Web technology must be assessed from a risk management perspective. If there are any doubts, do not release the information!

Release of information to foreign government service employees, international organizations and/or their representatives: Any military activity or defense contractor receiving a request for, or proposing to release information on this program will forward such requests/proposals to the OPR, after compliance with the following:

- Military activities will comply with the National Policy and Procedure for the Disclosure of Classified Military Information to Foreign Governments and International Organizations (NDP-1).

- Defense contractors will comply with the Department of State International Traffic in Arms Regulation (ITAR).

NOTE: Foreign national employees of the contractor or sub-contractor, including those possessing reciprocal clearances, are not authorized access to classified information resulting from or used in the performance of their contract unless authorized in writing by the OPR. Contractors shall ensure that this SCG, including all applicable standard security precautions and regulations identified in their DD Form 254, Contract Security Requirement, are complied with. Prime contractors are responsible for ensuring each of their subcontractors are aware of, and comply with, these requirements. Material proposed for release by subcontractors will be routed through their prime contractor.

Release of information to the United States Agencies: Requests will be submitted to the OPR.

Release of information at symposia, seminars, and conferences: Requests for such releases of classified information shall be submitted to the OPR for review and approval. Material will be submitted a minimum of six weeks prior to proposed release date in electronic format. Any information authorized for release will reflect that the work reported upon is sponsored by the DoD. If foreign nationals are expected to be present at such a conference, the provisions of paragraph 7 below must be followed.

Use of information or data classified by a foreign government: If information or data has been previously classified by a foreign government, this information or data will be classified at a level which will accord at least the same degree of protection as provided by the foreign government classification. This procedure will be adhered to even though a higher classification than that normally imposed by the U.S. for the same type of information will result.

7. FOREIGN DISCLOSURE

Foreign disclosure is the sharing of US classified information with foreign governments or international organizations in support of established or approved planned international programs. Any disclosure to foreign officials of information classified by this SCG shall be in accordance with the procedures set forth in DoD Directive (DoDD) 5230.11, DoDI 5230.27 and National Disclosure Policy (NDP-1). A foreign disclosure review shall be conducted prior to issuance of any solicitation. This review should result in a determination regarding which foreign governments and international organizations (and their industrial entities) will be permitted to participate in the solicitation.

General Release Guidance: Classified information is only released to properly cleared persons on a need-to-know basis and through government-to-government channels. It is the responsibility of the individual actually releasing the information to verify that the recipient is a foreign official authorized to receive classified information on behalf of his/her government or international organization and that information has been properly approved for release. JIEDDO personnel originating material classified by this guide will mark it as it is created in accordance with DoDI 5200.1-R, "Information Security Program," January 1997. JIEDDO information developed within combined spaces is presumed to be releasable to foreign nations represented in those spaces and should be marked "[CLASSIFICATION]//REL TO USA, [COUNTRY OR ORGANIZATION CODE]." When information is derived from multiple sources, the most restrictive handling and declassification instructions apply to the derived document. Classified information not explicitly marked releasable to a particular country shall not be released without proper authorization from the originating Foreign Disclosure Officer.

According to DoDD 5230.11, under conditions of actual or imminent hostilities such as Operation Iraqi Freedom or Operation Enduring Freedom, any unified or specified commander may disclose classified military information (CMI) through TOP SECRET to an actively participating allied force when support of combined combat operations requires the disclosure of that information. Under such circumstances, the Chairman, National Disclosure Policy Committee will issue further guidance determining any limitations that should be imposed on continuing disclosure of that information. When an authorized disclosure official (such as a Foreign Disclosure Officer (FDO)) has made a determination that CMI originated by JIEDDO is releasable under these conditions, the FDO should mark that information "[CLASSIFICATION]// REL TO USA, [COUNTRY OR ORGANIZATION CODE]," and forward an information copy to the JIEDDO FDO. A foreign disclosure review shall be conducted prior to issuance of any solicitation. This review should result in a determination regarding their foreign governments and

international organizations (and their industrial entities) permitted to participate in the solicitation.

8. FOREIGN GOVERNMENT INFORMATION AND FOREIGN MILITARY SALES

U.S. government information is furnished upon the condition that it will not be released to other nations without specific authority of the DoD of the United States. Subject release of information provides that individual or corporate rights originating the information will be provided substantially the same degree of security afforded it by the Department of Defense of the United States.

9. FOR OFFICIAL USE ONLY (FOUO) CAVEAT

For Official Use Only (FOUO) is not a security classification. FOUO information has not been given a security classification pursuant to the criteria in this SCG, but may be withheld from the public for one or more of the reasons cited in EO 12958, as amended, and DoDI 5200.1-R. Information so designated in this SCG that warrants FOUO markings will be handled and protected in accordance with regulations. The SCG for Freedom Of Information Act (FOIA) markings is intended solely as a guide. One, none or all of the suggested FOIA exemptions may apply to particular information depending on the particular facts of the information being protected or disclosed.

This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemption(s) . . . apply/applies.

ALL Freedom of Information Act (FOIA) exemptions identified in this SCG:

Number 1. Material appropriately classified by this SCG is similarly exempt from disclosure as National Security Information under FOIA.

Number 2. Related solely to the internal personnel rules and practices of the DoD or any of its components. Records containing or constituting statutes, rules, regulations, orders, manuals, directives, instructions, and security classification guides. This classification encompasses "High 2" information (i.e., information that would allow persons to circumvent or undermine JIEDDO's internal practices) and "Low 2" information (i.e., information of a trivial administrative nature.)

Number 3. Records protected by another law that specifically exempts the information from public release. Applicable to technical Controlled Unclassified Information (CUI).

Number 4. Containing trade secrets or commercial or financial information that a DoD Component receives from a person or organization outside the Government which is likely to cause substantial harm to the competitive position of the source, impair the Government's ability to obtain necessary information in the future, or impair some other

legitimate Government interest. Some examples: Commercial or financial information received in confidence in connection with bids, contracts, or proposals; statistical data and commercial or financial information concerning contract performance, income, etc.; personal statements given in the course of inspections, investigations, or audits; financial data provided in confidence by private employers in connection with locality wage surveys; scientific and manufacturing processes or developments concerning technical or scientific data or other information submitted with an application for a grant or with a report while research is in progress; technical or scientific data developed by a contractor or subcontractor exclusively at private expense and technical or scientific data developed in part with federal funds and in part at private expense; computer software which is copyrighted; or, proprietary information submitted strictly on a voluntary basis.

Number 5. Subjective evaluations that are reflected in records pertaining to the decision-making process of an agency. Examples are: advice, suggestions or evaluations prepared on behalf of the DoD; non-factual portions of evaluations by DoD component personnel of contractors and their products; information of a speculative, tentative or evaluative nature; trade secret or other confidential research development; and portions of official reports on inspection, reports of the IG, audits, investigations, or surveys pertaining to safety, security, or the internal management, administration or operation of one or more DoD components.

10. DISTRIBUTION STATEMENT

Distribution statements are required to be placed on all technical documents no matter if they are classified or unclassified. Export controlled warning notices will be applied only to technical documents containing critical technology. These notices will be placed on the front cover or first page of the document. When possible, parts that contain information creating the requirement for a distribution statement or other warning notice shall be prepared as an appendix to permit broader distribution of the basic document.

Technical documents contain information (experimental, developmental, engineering works) that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The information may be in text, graphic, or pictorial form.

The following statements will be applied to all technical documents as defined as above:

DISTRIBUTION STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD contractors (fill in reason) (date of determination). Other requests for this document shall be referred to the JIEDDO Security Office.

Reasons for applying distribution D:

Foreign Government Information: To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information.

Administrative or Operational Use: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Software Documentation: Releasable only in accordance with DoD Instruction 7930.2, Automatic Data Processing (ADP) software exchange and release.

Transfer of data from SIPR to a CD: Transfer of data from SIPR to a CD: Any data that needs to be transferred from SIPR to a CD must be done in accordance with US CYPERCOM CTO 10-133. Currently J6 and STRATCOM are the only authorized divisions that transfer data. All CD with SIPR Data or higher must bear the proper security marks (AR 380-5). Any CD(s) that needs to be mailed/hand carried out of the Polk building must go through JIEDDO Security. For further guidance, please contact JIEDDO Security.

Critical Technology: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of DoDD 5230.25. Apply the following notice to the front cover or title page:

Warning – This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, USC, Sec 2751 etc) or the Export Administration Act of 1979, as amended (Title 50, USC, App 2401 etc). Violations of these export laws are subject to severe criminal penalties.

Specific Authority: To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as executive orders, classification guides, DoD or DoD component regulatory documents. When filling in the reasons, cite "Specific Authority (identification of valid documented authority),"

At times, the application of a different distribution statement may be necessary to facilitate sharing between U.S. government agencies (Distribution Statements B and C) or to limit dissemination based upon the Director's discretion (Distribution Statement F). Further exceptions for the use of another distribution statement shall be submitted to the JIEDDO Security Office, in writing, with justification.

11. DISCLOSURE OF INTELLIGENCE/THREAT INFORMATION

Data or information relating to threat systems or other intelligence derived material must bear the security markings of that intelligence/threat material. All dissemination of intelligence / threat information is controlled by the Director, COIC. Intelligence/threat information may be reproduced, released to subcontractors, provided instructions, and procedures approved by the COIC Director. Intelligence/threat information may be reproduced, released to subcontractors, provided instructions, and procedures approved by the Senior Intelligence Officer (SIO) are followed. Questions regarding such releases shall be referred to the SIO.

12. LOSS, COMPROMISE, OR SUSPECTED COMPROMISE

Report the loss, compromise, or suspected compromise of classified JIEDDO information or material to the JIEDDO Security Office, 703-601-4744, within 24 hours of the incident.

13. COMPILATION OF INFORMATION.

In some circumstances, classification may be required if the compilation of unclassified items of information provide an inference that warrants classification. Similarly, a higher classification may be assigned to a compilation of information if the compilation provides an added factor that warrants higher classification than that of its component parts. Classification on this basis will be used sparingly, and complete justification of this classification method will be stated on the title or first page of the document. The classification and marking process is as follows:

- When a document comprises individually unclassified items of information is classified, by compilation, the overall classification shall be marked conspicuously at the top and bottom of each page and the outside front and back covers (if applicable). An explanation of the basis for classification by compilation shall be placed on the face of the document or included in the text.

- If portions, standing alone, are unclassified, but the document is classified by compilation or association, those portions shall be marked "U" and the document and pages shall be marked with the classification of the compilation. An explanation of the classification or the circumstances involved with association must be included.

- If individual portions are classified at one level and the compilation is a higher classification, each portion shall be marked with its own classification and the document and pages shall be marked with the classification of the compilation. An explanation of the classification by compilation is required.

14. REASONS FOR CLASSIFYING

The reasons for classifying information in this SCG are in accordance with Part I, Section 1.4, Executive Order 12958 (as amended). They are:

1.4a – Military plans, weapons systems, or operations
1.4b – Foreign government information
1.4d – Foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to national security
1.4 e – Scientific, technological, or economic matters
1.4 g – Vulnerabilities or capabilities of the system, installation, projects, or plans relating to the national security

15. DEFINITIONS

Classified Performance Capabilities or Limitations: Information that if disclosed would;

1) damage national security through facilitating adversary denial, degradation, disruption, deception, or destruction of mission essential or critical system(s), or
2) would require major modifications to an acquisition program or operational system to maintain the technological advantage of the system during its projected operational life time.

Compromise a Future Capability: Anything not in the inventory now and is planned to be developed; not a current capability. Applies to research, development and acquisition efforts.

Confidential: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security that the original classification authority is able to identify or describe.

Critical Information: TBD by the supported organization. Different organizations may deem information differently as to its criticality. Determination and defense of information as critical is up to the supported organization.

Critical Program Information (CPI): Information, technologies, or systems that, unto themselves, if compromised would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction.

Effectiveness of Forces: TBD by supported organization. Usually refers to squad to division level. Different organizations may deem information differently as to its impact on the effectiveness of forces. For example; information that may impact the effectiveness of a Special Forces unit compared to a Battalion is potentially considerable. Determination and defense of information is up to the supported organization.

Effectiveness of Major Forces: TBD by supported organization. Usually refers to theater level; unified command; combination of Military Departments (MILDEPS). Different organizations may deem information differently as to its impact on the effectiveness of major forces. Determination and defense of information is up to the supported organization.

Enhanced System Capability: An improvement over existing performance or capabilities found on similar systems.

Low- Level Intelligence Collection Capability: Focused on low- level counterintelligence, Human Intelligence (HUMINT) sources, e.g., bartender, "beat cop," or low- level detection capability, e.g., unattended ground sensors.

Mission Critical: A mission essential item whose disruption or destruction immediately degrades the ability of the force to command, control, or effectively conduct combat operations. For example, disruption or destruction of the mechanism used to fuse a system-of-systems (e.g., C4ISR) would result in the immediate inability for the separate system to act in concert as a system-of-systems.

Mission Essential: Those items required to support approved emergency and/or war plans, and where those items are used to:

1) destroy the enemy or the enemy's capacity to continue war;
2) provide battlefield protection of personnel;
3) communicate under war conditions;
4) detect, locate, or maintain surveillance over the enemy;
5) provide combat transportation and support of men and materiel; and/or
6) support training functions.

National Military Objectives: Protect the United States against external attacks and aggression; prevent conflict and surprise attack, and prevail against adversaries. These are the ends of the strategy and help to assure allies and friends, dissuade adversaries, and deter aggression and coercion while ensuring the armed forces remain ready to defeat adversaries should deterrence and dissuasion fail. They serve as benchmarks to assess levels of risk and help to define the types and amounts of military capabilities required.

National Objectives (for DoD): The aims derived from national goals and interests, toward which a national policy or strategy is directed and efforts and resources of the nation are applied.

National Security Strategy (for DoD): The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national security. Also called national strategy or grand strategy.

NOFORN: (NOT RELEASABLE TO FOREIGN NATIONALS) Under authority of Director of Central Intelligence, this marking is used for identified *classified intelligence* that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens without permission of the originator and in accordance with provisions of DCID 6/7 and NDP-1. Cannot be used with REL TO [country codes] or EYES ONLY on page markings (when a document contains both NOFORN and REL TO or NOFORN and EYES ONLY portions, NOFORN takes precedence for the markings at the top and bottom of the page).

Reveal a National Security Objective: Fact of statement that would reveal an undisclosed objective or intention— that is covert in nature. Details of how we plan to achieve national security objectives (primarily planning oriented).

Secret: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Senior Leadership: President of the US (POTUS); Cabinet Members, Pentagon Senior Leadership, etc.

Sensitive Information: TBD by the supported organization. Different organizations may deem information differently as to its sensitivity. Determination and defense of information as sensitive is up to the supported organization.

Sensitive Intelligence Collection Capability: To be determined by the user or developer of that capability.

Significant Impairment: Any characteristic or concept, design or component that offers a technical disadvantage of enough magnitude to be potentially disruptive in an operational or advanced system.

State of the Art: The highest level of development, as of a device, technique, or scientific field, achieved at a particular time. For a system or technology that has no known baseline to determine its relative level of development, the very nature of it being the first of a kind, makes it state of the art.

Strategic Advantage: Operational superiority provided via military instruments that enables one nation or group of nations effectively to control the course of a military or political situation beyond a battle or engagement.

Strategic Disadvantage: Inverse of strategic advantage (see above definition).

Tactical Advantage: Operational superiority provided via unit and system performance and capabilities during battles and engagements planned and executed to accomplish military objectives assigned to tactical units or task forces.

Tactical Disadvantage: Inverse of tactical advantage (see above definition).

Threaten the Country's Ability to Wage War: Identification of details of war plans that would reveal overall objectives or intentions.
Top Secret: Shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the original classification authority is able to identify or describe.

Weaken the Country's Ability to Wage War: Identification of specific details of war plans in a theater of operation including use of tactical capabilities and mission essential items.

Significantly Weaken the Country's Ability to Wage War: Identification of specific dependencies and objectives in a theater of operation or sub area of a Unified Command to include strategic capabilities and mission critical items.

Threaten the International Position of the US: Damage US credibility with a foreign government.

Weaken the International Position of the US: Negative impact to the international position of the US and its ability to negotiate with foreign governments.

Significantly Weaken the International Position of the US: Inability of the US to successfully negotiate with a foreign government for a significant period of time.

Unique and Fragile Intelligence Collection Capability: To be determined by the user or developer of that capability.

Only trained FDOs who have been issued a Delegation of Disclosure Authority Letter (DDL) can authorize the disclosure or release of classified military information to authorized representatives of foreign governments or international organizations as outlined in this guide.

ADMINISTRATION DATA

Element	Level	Duration	Remarks
JIEDDO Goal, Mission and Purpose			
JIEDDO mission	U		Public Release and Distribution Statement A applies for the following description: JIEDDO shall focus (lead, advocate, coordinate) all Department of Defense actions in support of Combatant Commanders and their respective Joint Task Forces' efforts to defeat improvised explosive devices as weapons of strategic influence. (DoDD 2000.1E)
JIEDDO organizational structure (Line and block chart identifying position only)	U		
JIEDDO organizational structure (Line and block chart identifying personnel by name)	U		Mark and handle as FOUO, FOIA exemption 2 applies.
JIEDDO Goals and Objectives	U		Mark and handle as FOUO, FOIA exemption 2 applies. Specific technological goals and objectives associated with real or postulated threats will be addressed by other portions of this SCG
JIEDDO Resources			
Financial plans	U		
Financial plans with classified program Names	U		Classify as directed by program security classification guide, FOIA 1(b)(2)(a).
JIEDDO budget	U		
Cost, pricing, or funding for individual systems, subsystems, or components	See Remarks		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies. FOIA exemption 4 may apply to certain proprietary or trade secret information provided by vendors.

			If individual project budget reveals a sensitive relationship between the JIEDDO and other DoD organizations, US government organizations, or a foreign government or foreign owned company then classify in accordance with the guidance provided by the other organization, government, or the contractor relationship portion of this document.
Budget levels for projects	See Remarks		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies. If individual project budget reveals a sensitive relationship between the JIEDDO and other DoD organizations, US government organizations, or a foreign government or foreign owned company then classify in accordance with the guidance provided by the other organization, government, or the contractor relationship portion of this document..
Production quantities and delivery rates	U		If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Manpower, overall by year, category, skill, and system	U		
Manpower, overall by year, category, skill, system, and individual name	U	If classified, declass in accordance with proponent SCG.	Mark and handle as FOUO, FOIA exemption 2 applies.
Identification of a particular installation, facility or range associated with the JIEDDO	U-S		Classify as directed by program security classification guide.
Aggregate number of C-IED systems deployed in a particular theater of operation or to a particular unit	See Remarks		Peacetime Situations: Derivative according to documents such as Table or Organization and Equipment. Combat Situations: Derivative according to operational SCG such as MNF-I or OEF SCG.
JIEDDO Schedules			
Organization master schedule	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Specific program/project status	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.
Development milestones	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.

Procurement milestones	U-S		Mark and handle as FOUO, FOIA exemption 2 applies.
Contractor Relations			
Partial or full list of contractors producing or procuring IED defeat systems or component pieces	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Data on parts, accessories and equipment available in the open market or produces for commercial use not tied or related to IED defeat capabilities	U		Public release and distributions statement A applies.
DD 254s	U - S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Statements of work	U - S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Organization Security			
Results of program protection risk management processes / analysis	See Remarks		Mark and handle as FOUO, FOIA exemption 2, 5 applies. Specific information may be derivatively classified from documents such as threat assessments, etc.
Details of specific protection measures associated with the JIEDDO Note: Specific protection measures are those relative to the JIEDDO and not generalized guidance	See Remarks (U-S)		Mark and handle as FOUO, FOIA exemption 2 applies. RAM Measures at a minimum is SECRET Specific information may be derivatively classified from documents such as threat assessments, etc.

JIEDDO OPERATIONS

Element	Level	Duration	Remarks
General information regarding the requirements for the JIEDDO and IED defeat systems	See Remarks	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical requirements associated with a specific system, subsystem or component	U-S	Declassify 10 years from date of creation	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Identification of key performance threshold/objective parameters associated with the JIEDDO and specific IED defeat system, subsystem or component	See Remarks	Declassify 10 years from date of this document	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Operational capabilities/shortfalls	See Remarks **(U-TS)**	Declassify 10 years from date of this document	Classify in accordance with the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and/or 5 applies.
IED- Related SIGACTS	See Remarks (U-TS)		Classify in accordance with SCG for the program or system. All theater derived SIGACTS are SECRET.
JIEDDO specific tactic's techniques and procedures (TTPs)	See Remarks (C-TS)	Declassify 10 years from date of this document	Classify in accordance with the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies.
JIEDDO CONOPS	U-S	Declassify 10 years from date of this document	Classify in accordance with SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies.
Movement of JIEDDO related personnel and equipment.	See Remarks		If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.) If

Formatted: Font: Bold

			UNCLASSIFIED FOIA 2 potentially applies.
Field team locations	See Remarks		If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.).
Field Team Composition, disposition, and strengths	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2.
Field Team requirements and mission	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). Specific information not covered in an operational classification guide; classify in accordance with the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2.
Analysis products by JIEDDO intelligence analysts	See Remarks		Classify in accordance with the applicable Intelligence Community classification guide. If no guidance is available refer to DoDD 5240.08 (DOD CI SCG, December 2005, if UNCLASSIFIED FOIA 2, 4 and 5 applies).
JIEDDO intelligence requirements	S	Declassify 10 years from date of this document	Classify in accordance with current markings or the SCG for the operation, program or system, (if UNCLASSIFIED FOIA 2, 4 and 5 applies).
Specific IED- related system employment locations	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.) (If UNCLASSIFED FOIA 2, 4 and 5 applies).
Specific IED- related system employment methods	See Remarks	Declassify 10 years from date of this document	If supporting combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). Specific information not covered in an operational or system specific classification; classify in accordance with the SCG for the program or system. Classification of employment locations may be classified a higher levels or within compartmented channels based upon operational guidance.

			If UNCLASSIFED, mark and handle as FOUO, FOIA exemption 2, 4 and 5 potentially applies.
IED lessons learned	U-S	Declassify 10 years from date of this document	If resulting from combat operations, refer to applicable operational classification guide (MNF-I, OEF, etc.). For JIEDDO specific developed lessons learned treat as: Classify in accordance with current classification or the SCG for the program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 and/or 5 applies.
Initial Review Group (IRG) internal decision- making processes and results	U-S	Declassify 10 years from date of this document	Classify in accordance with current markings or the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Technology Review Group (TRG) internal decision- making processes and results	U-S	Declassify 10 years from date of this document	Classify in accordance with current markings or the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
JIEDD Requirements, Resources and Acquisition Board (JR2AB) internal decision making processes and results	U-S	Declassify 10 years from date of this document	Classify in accordance with current markings or the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Joint Integrated Product Team internal decision- making processes and results	U-S	Declassify 10 years from date of this document	Classify in accordance with current markings or the SCG for the operation, program or system. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.

C-IED Operational/Intelligence Integration Center (COIC)

For Further Information Refer to Annex A of this Classification Guidance

COIC mission	U		

RED AND BLUE TEAM ACTIONS

Element	Level	Duration	Remarks
Fact that JIEDDO performs red teaming and blue teaming	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Red team and blue team reports	See Remarks		Results are to be classified at the same level as the items or systems being Red Teamed or Blue Teamed – classify in accordance with information revealed. If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as derivative from other sections of this SCG. Classification of red team and blue team plans and results is dependent on the security classification of the information involved.
Field team prototypes of possible new threat modes or techniques	See Remarks		Prototypes without accompanying explanatory information will be handled as FOUO. FOIA 4 potentially applies. When associated with specific Red Team and Blue Team reports classify at the same level as the associated report.
Limitations or vulnerabilities associated with IED defeat systems or subsystems revealed by Red Teaming or technical gaming	See Remarks	Declassify 10 years from date of this document	Classify according to the level of information revealed through the association of limitations or vulnerabilities of specific IED defeat systems. If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as: CONFIDENTIAL if loss of information would reveal or

			compromise a future capability. SECRET if details would lead to loss of research, development and engineering; scientific, or technical information that would lead to a tactical disadvantage. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.

JIEDDO SYSTEM AND SUBSYSTEM PERFORMANCE AND CAPABILITIES

This section applies to all IED detection and defeat systems and subsystems.
(Many such systems fall under a different Original Classification Authority than JIEDDO owned information – i.e. Warlock Red falls under the authority of PM SW and PEO IEW&S and therefore all classification determinations for this system are found in the Joint counter radio controlled improvised explosive service electronic warfare Program Security Classification Guide) (CREW)

Element	Level	Duration	Remarks
General information regarding the capabilities of IED defeat systems or subsystems	U		General information is that which can be found in unclassified requests for proposals and approved JIEDDO press releases and media guidance, and documents marked with FOIA distribution statement A.
Specific details regarding the capabilities of IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 or 5 applies.
Emerging IED defeat capabilities or systems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
(CREW) System or Subsystem	See Remarks		For guidance on all CREW system, refer to the Joint Counter Radio Controlled Improvised Explosive Service Electronic Warfare Program Security Classification Guide, 8 August, 2006 (OPNAVINST 5513.8B-88). If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Maximum range of detection / defeat for	See Remarks	Declassify 10 years	If system specific classification guidance exists, then classify

IED defeat system or subsystem		from date of this document	in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Detection rates	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
The fact that specific IED defeat systems will be used to protect specifically named VIP's	See Remarks (S-TS)	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. The general statement that C-IED systems are used for VIP protection is UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 and/or 5 applies. The fact C-IED systems are being used to protect specific VIPs is classified SECRET based on the program SCG, the loss of information could lead to a tactical disadvantage. Classification of C-IED systems being used to protect specific VIPs may be classified at higher levels or within compartmented channels based upon operational guidance.
Effectiveness of IED defeat systems or subsystems against general threats	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. General categories of threats that C-IED systems are designed to counter (e.g. car alarms, cell phones, etc) UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Effectiveness of IED defeat systems or subsystems against specific threats	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific system Concept of Operations (CONOPS)	See Remarks (C-S)	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA

			exemption 2, 4 or 5 applies.
Specific system tactics, techniques. procedures (TTPs)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Frequency ranges when expressed in general terms (such as Band A / Band B)	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Frequency bands expressed in general terms that do not reveal actual operating parameters is UNCLASSIFIED.
Frequency bands associated with specific IED defeat systems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. Listing of actual operating frequencies, frequency bands, or entire spectrum coverage is SECRET – the loss of information could lead to a tactical disadvantage. If UNCLASSIFIED, FOIA 4 potentially applies.
Antennas associated with IED defeat systems or subsystems	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. The fact that specific antennas are being used for C-IED systems is UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies. If performance characteristics of an antenna are classified, then classify in accordance with the applicable SCG.
IED defeat system or subsystem reliability, maintainability, and supportability	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Technical details of signal processing or jamming techniques / parameters	See Remarks	Declassify 10 years from date of this	If system specific classification guidance exists, then classify in accordance with that guidance.

		document	If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Threat characteristics that are used to determine which IED defeat system or subsystem to employ	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
RF Output power or other information that would reveal effective range of operation	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Input sensitivity or other information that would reveal system or subsystem detection range	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Interoperability between various IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Interoperability between IED defeat systems or subsystems and other equipment (communication equipment, weapons systems, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.

JIEDDO RELATED HARDWARE / SOFTWARE

(Some Hardware and Software falls under a different Original Classification Authority than JIEDDO owned information – i.e. Warlock Red falls under the authority of PM SW and PEO IEW&S and therefore all classification determinations for this system are found in the Joint Counter Radio Controlled Improvised Explosive Service Electronic Warfare Program Security Classification Guide)

Element	Level	Duration	Remarks
Technology Integration			
General description of technologies being considered for use by JIEDDO Note: Technologies that have actually been selected for use by JIEDDO are covered in the respective SCG	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as: UNCLASSIFIED - Mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical details of technologies being considered for use by JIEDDO Note: Technologies that have actually been selected for use by JIEDDO are covered in the respective SCG	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Design Details			
General information regarding IED defeat systems or components of systems	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Design specifications of IED defeat systems or components of systems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Specific technical details regarding IED defeat systems or components of systems (antennas, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Network architecture system view	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Network architecture technical view	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Network architecture network functions	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Software architecture	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Software source code	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Information assurance technical details (To include Cross Domain Guard, Network Intrusion Detection System, Key Fill Bus, firewall, and switches)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2, 4 or 5 applies.
Cryptographic capabilities and equipment	See Remarks		Contact OPR COMSEC material and controlled cryptographic items shall be handled, marked and safeguarded in accordance with policies and procedures of the National Security Agency. If UNCLASSIFIED, mark and handle as FOUO, FOIA

			exemption 2, 4 or 5 applies.
Modeling and Simulation			
Fact that modeling and simulation is used for design and validation of a specific system, subsystem or component	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as UNCLASSIFIED - Mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Operational parameters for specific modeling and simulation at the force, system, subsystem or component level	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Details of specific items in the modeling and simulation database	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Results of the modeling and simulations	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Commercial Off the Shelf (COTS) / Government Furnished Equipment (GFE)			
Fact that the JIEDDO uses COTS/GFE systems	U		Public Release and Distributions Statement A applies.
Association of COTS/GFE used on a particular IED defeat system, subsystem, or component	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Mark and handle as FOUO, FOIA exemption 4 potentially applies.
Modification of COTS/GFE	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Unusual or unique application of GFE	See Remarks	Declassify 10 years	If system specific classification guidance exists, then classify

		from date of this document	in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details about modification of COTS/GFE	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Manufacturing / Fabrications			
Fact that unique / non-traditional manufacturing processes are used to develop IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details of unique / non-traditional manufacturing processes used to develop IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Integration			
Fact that unique / non-traditional integration processes are used to develop IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Identification of unique / non–traditional integration techniques with specific IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Technical details of unique / non-traditional integration techniques relative to IED defeat systems, subsystems, or components	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 3, 4 and 5 applies.
External / Internal Views			
External view of IED defeat systems, subsystems, or components (including	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance.

drawings, photographs, etc.)			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4.
Internal view of IED defeat systems, subsystems, or components (Including technical drawings of systems, components such as wiring plans, blueprints, and section cutaways)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Anti-Tamper			
General information regarding the fact that anti-tamper is used on IED defeat systems, subsystems, or components	U		
Technical details regarding implementation of anti-tamper to deter / delay attempts at reverse engineering of hardware / software of IED defeat systems, subsystems, or components	See Remarks		Refer to the Anti Tamper SCG, dated 1 March 2001. If UNCLASSIFIED, FOIA exemption 2, 4 or 5 potentially applies.

VULNERABILITIES AND WEAKNESSES

Element	Level	Duration	Remarks
General information regarding vulnerabilities and limitation of IED defeat systems or subsystems (i.e. information found via open sources related to common vulnerabilities such as the statement that "coalition troops are vulnerable to VBIED attacks")	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Combination of open source material may classify information General information not covered in a component classification guide is treated as: UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and 5 applies.
Details of specific operational limitations and vulnerabilities of IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Identification of system susceptibilities in the presence of a validated threat to a specific IED defeat system or subsystem	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

			If UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Technical details of specific countermeasure employed (e.g. ECM, Anti-Tamper, Signature Management, etc)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, FOIA, exemption 4 or 5 potentially applies.
Effectiveness of specific countermeasures	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFED, FOIA exemption 4 or 5 potentially applies.
Information regarding signals or initiation means which may not be detected or which may be immune to specific IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFED, FOIA exemption 4 or 5 potentially applies.

INDUSTRY TEST AND EVALUATIONS

Element	Level	Duration	Remarks
Details of IED defeat system or subsystem test plan	See Remarks		Testing is to be classified at the same level as the item being tested – classify in accordance with information revealed. If system specific classification guidance exists, then classify in accordance with that guidance. If, UNCLASSIFIED, FOIA exemption 4 or 5 potentially applies.
Identification of specific dates for IED defeat systems or subsystem tests	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Identification of specific test locations associated with IED defeat systems or	U		Mark and handle as FOUO, FOIA exemption 2 applies.

subsystems			
Identification of specific or specialized test instrumentation or equipment associated with IED defeat systems or subsystems	See Remarks	Declassify 10 years from date of this document	Classify according to the level of information revealed through the association of specialized test equipment with specific IED Defeat systems. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Predicted test data	See Remarks		Testing is to be classified at the same level as the item being tested – classify in accordance with information revealed. Predicted test data that provides specific performance and capability data on IED defeat System or Subsystem shall be classified in accordance with that component Security Classification Guide. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Raw test data	See Remarks		Testing is classified at the same level as the item being tested – classify in accordance with information revealed. Raw data that provides specific performance and capability data on IED defeat System or Subsystem shall be classified in accordance with that components Security Classification Guide. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Reduced test data	See Remarks		Testing is classified at the same level as the item being tested – classify in accordance with information revealed. Reduced test data that provides specific performance and capability data on IED defeat System or Subsystem components shall be classified in accordance with that components Security Classification Guide. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.

TRAINING

Element	Level	Duration	Remarks
Training location specific to the JIEDDO and IED defeat systems, subsystems, or components	U		Mark and handle as FOUO, FOIA exemption 2 applies.
Training that reveals specific system information (e.g. design, development, capabilities, vulnerabilities, etc.) Note: This element includes live training, virtual training, and constructive training.	See Remarks	Declassify 10 years from date of this document	Classify in accordance with the level of information revealed during the training. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 4 and/or 5 applies.
Training Aids (Includes both IED training devices and C-IED training devices)	U		If, UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.

MAINTENANCE

Element	Level	Duration	Remarks
Location of specialized maintenance organizations associated with the JIEDDO and IED defeat systems, subsystems, or components	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. Specific information not covered in a component classification guide is treated as UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Association of maintenance equipment or tools that may reveal specific system information	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Maintenance that reveals specific system information (e.g. design, development, capabilities, vulnerabilities, etc.)	See Remarks	Declassify 10 years from date of this document	If system specific classification guidance exists, then classify in accordance with that guidance.

			If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 or 4 applies.
Field level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Intermediate level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.
Depot level maintenance	See Remarks		If system specific classification guidance exists, then classify in accordance with that guidance. If UNCLASSIFIED, mark and handle as FOUO, FOIA exemption 2 applies.

SECTION X – APPLICABLE SECURITY CLASSIFICATION GUIDES

Deputy Secretary of Defense Memorandum Dated 24 Apr 2006, SUBJECT: Policy on Discussion of IEDs and IED-Defeat Efforts in Open Sources

Operational Capabilities Infusion Team (OCIT) Technology Efforts In Support of the Detection and Defeat of Improvised Explosive Device (IED) Classification Guide (Revised 10 March 2004)

MNF-I / MNC-I Security Classification and Marking Guide, Version 5, Change 1, 05 Aug 2005

DoD Security Classification Guide Operation Enduring Freedom, Operation Noble Eagle, 28 Mar 2002

USCENTCOM Security Classification Guide 0501, Dated: 9 June 2005

Classification Guidance for EC-130H and EA-6B Counter-RCIED Operations in Operation IRAQI FREEDOM

Classification Guidance for EC-130H and EA-6B Counter-RCIED Operations in Operation ENDURING FREEDOM

Counter Radio Controlled Improvised Explosive Service Electronic Warfare Program Security Classification Guide, 8 August, 2006 (OPNAVINST 5513.8B-88)

SECTION XI REFERENCES

1. Executive Order 12958, as amended, 5 Jan 2006

2. AR 380-5, "Department of the Army Information Security Program," 14 Jan 2006

3. DOD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," Jan 1995, Change 1, 31 Jul 1997; Change 2, 28 Feb 2006

4. AR 25-55, "Department of the Army Freedom of Information Act Program." 15 Jan 2006

5. DOD Directive 5230-25, "Withholding of Unclassified Technical Data from Public Disclosure," 6 Nov 1984; Change 1, 8 Apr 1995

6. DOD Directive 5230-24, "Distribution Statements on Technical Documents." 8 Apr 2004

7. DOD Pamphlet 5230.25-PH, "Control of Unclassified Technical Data with Military or Space Application," 15 Apr 2004

8. DOD 5200.1-R "Information Security Program," Feb 2009

9. DOD 5230.9 "Clearance of DoD Information for Public Release," 22 Aug 2008

10. DOD 5230.11 "Disclosure of Classified Military Information to Foreign Governments and International Organizations," 7 Feb 2006

11. DODI 5230.27 "Presentation of DoD-related Science and Technical Papers at Meetings, 6 Oct 1987