HEADQUARTERS UNITED STATES CENTRAL COMMAND
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

REGULATION
Number 380-14 15 June 2012

Security
CLASSIFICATION GUIDE

TABLE OF CONTENTS



*This regulation supersedes CCR 380-14, 26 Feb 10. (See "Summary of Changes" on page 8-1.)

TABLE OF CONTENTS (Continued)

APPENDICES (Continued) PAGE

THIS PAGE INTENTIONALLY LEFT BLANK

# CHAPTER 1
# GENERAL

1-1. PURPOSE. This guide establishes the basic policies for proper marking, 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), its components and units assigned to or operating in the USCENTCOM Area of Responsibility (AOR).

1-2. APPLICABILITY. This guide applies to Headquarters, USCENTCOM, its components, and those government agencies (civilian contractors and personnel) involved in the activities of USCENTCOM, and any units or subordinate commands operating in the USCENTCOM AOR.

1-3. AUTHORITY. The Original Classification Authority (OCA) for this guide is Commander, USCENTCOM. This classification guide reflects changes required by Executive Order (EO) 13526 dated 29 December 2009, Classified National Security Information", the Information Security Oversight Office (ISOO) Implementing Directive (32 CFR Parts 2001 and 2003), subsequent ISOO Notices, Intelligence Community Directive (ICD) 710 Classification and Control Markings System dated 11 September 2009, ICD 208 Writing for Maximum Utility dated 17 December 2008, the Controlled Access Program Coordination Office's (CAPCO) Authorized Classification and Control Markings Register dated 31 May 2011, and the CAPCO Intelligence Community Classification and Control Markings Implementation Manual dated 31 May 2011; and Department of Defense (DoD) Regulation 5200.1-R, Information Security Program, January 1997. Changes in classification markings are required in accordance with EO 13526 and ICD 710, Classification and Control Markings System which are implemented through the Director of National Intelligence's CAPCO Authorized Classification and Control Classification Markings Register and the CAPCO Intelligence Community Classification and Control Markings Implementation Manual. The classification authority for information covered under this guide shall be cited as shown below, along with the appropriate declassification instructions.

Classified By: Joe Carver, Director
Derived From: Department of Good Works SCG dated June 27, 2010
Declassify On: 20151231(This date is dependent upon the guidance found in appendices A-V of this guide)

1-4. OFFICE OF PRIMARY RESPONSIBILITY (OPR). The USCENTCOM Special Security Office (SSO) issues this guide. Address inquiries concerning content and interpretation, as well as any recommendations for changes to:

USCENTCOM Special Security Office
7115 South Boundary Blvd
MacDill AFB, FL 33621-5101

1-5. INDIVIDUAL RESPONSIBIITIES. Individuals are responsible for ensuring information is properly protected and classified appropriately. Over classification of information hinders the

timely sharing of information and mission accomplishment. Originators of information must ensure all documents are properly marked and written for release. Classification and control requirements apply to information regardless of the medium (e.g., text, images, graphics, and electronic documents (including web pages, e-mails, cables disseminated via message-handling systems, wikis, and blogs). Portion markings shall be used on all classified information unless a waiver has been obtained in accordance with guidance from the ISOO; heads of Intelligence Community elements may submit requests for waivers to markings, formats, or authorized abbreviations in writing to CAPCO for Director of ODNI/ONCIX/SEC/SSD consideration. Classified information must have: (1) The highest classification level of information contained in the document and applicable control markings on the top and bottom (header and footer; banner line) of each page or slide; (2) classification portion marks; (3) the classification authority block; and (4) Date of origin of the document. Originators shall include a point of contact and contact instructions at the end of all classified products to expedite decisions on information sharing. Unclassified information with control markings must have: (1) The highest classification level of information contained in the document and applicable control markings on the top and bottom (header and footer; banner line) of each page or slide and (2) classification portion marks.

1-6. CLASSIFICATION CHALLENGES. If at any time, any of the security classification guidance undergoes a challenge, the items of information shall continue to be protected at the level prescribed by this guide until an OCA has made a final determination. Requestors of information and authorized holders of information shall seek to resolve issues at the lowest possible level. Classification challenges should follow the procedures provided in Section 1.8 of EO 13526, as well as implementing procedures established in accordance with this Executive Order and Director of National Intelligence (DNI) guidance.

# CHAPTER 2
# TYPES OF INFORMATION

2-1. U.S. classification markings (TOP SECRET, SECRET, CONFIDENTIAL) are used in the header and footer (top and bottom) of each page and each product. The classification must be spelled out in full and may not be abbreviated in the banner line. A product may have only one classification on the top and bottom. FOR OFFICIAL USE ONLY (FOUO). FOUO is unclassified DoD information that has not been given a security classification pursuant to the criteria of EO 13526, but which may be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more Freedom of Information Act (FOIA) Exemptions in DoD 5400.7-R. No other material shall be considered FOUO. Unclassified information with control markings such as FOUO must have: (1) The highest classification level of information contained in the document and applicable control markings on the top and bottom (header and footer; banner line) of each page or slide and (2) classification portion marks.

2-2. CLASSIFIED INFORMATION. Classified information is information that has been determined by an OCA or through derivative classification to pose a risk to national security if not protected properly. The United States (U.S.) government recognizes three levels of classification.

a. TOP SECRET - Assigned when the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security that the OCA is able to describe.

b. SECRET - Assigned when the unauthorized disclosure could reasonably be expected to cause serious damage to the national security that the OCA is able to describe.

c. CONFIDENTIAL - Assigned when the unauthorized disclosure could reasonably be expected to cause damage to the national security that the OCA is able to describe.

2-3. SENSITIVE COMPARTMENTED INFORMATION (SCI). SCI is information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products. These special community controls are formal systems of restricted access established to protect the sensitive aspects of sources, methods and analytical procedures of foreign intelligence programs. The Chief, SSO is the office responsible for indoctrination in SCI and ensuring compliance with all applicable regulations and directives.

2-4. SPECIAL ACCESS PROGRAM (SAP) INFORMATION. SAP involves activities that fall within the statutory authority and responsibility of the DNI. Within these provisions, only those programs that require, as a condition of access, the signing of a nondisclosure statement are considered SAPs. SAPs are given the status of SCI compartments and sub compartments in terms of the minimum required security levels necessary for their protection. Within USCENTCOM the Director of Operations is responsible for the administration and indoctrination of personnel deemed eligible.

2-5. NORTH ATLANTIC TREATY ORGANIZATION (NATO) AND FOREIGN GOVERNMENT INFORMATION (FGI)

a. NATO Information. NATO classified information will be safeguarded in accordance with (IAW) U.S. Security Authority for NATO Instruction I-69. USCENTCOM Command & Control, Communications & Computer Systems Directorate (CCJ6) is responsible for ensuring compliance with network handling instructions for NATO material. SSO will indoctrinate those personnel requiring NATO access.

b. FGI. Under E.O. 13526, and ISOO Implementing Directive (32 CFR Parts 2001 and 2003), Foreign Government Information is defined as (1) Information provided to the U.S. government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; or (2) Information produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the arrangement, or both, are to be held in confidence; or (3) Information received and treated as "Foreign Government Information" under the terms of a predecessor order. During the course of exercises and operations, USCENTCOM receives information from foreign governments. This material is required to be protected at the equivalent level of U.S. classification. U.S. personnel receiving FGI must be cleared to the appropriate level of the information received. FGI markings are used on U.S. products to denote the presence of foreign-owned or foreign-produced information in both the portion markings and on the top and bottom of the page or product. Use FGI plus the trigraphic country codes listed in ISO 3166 or the tetragraphic codes for international organizations or groups of countries as listed in the CAPCO Register APPENDIX A and APPENDIX B, unless the very fact that the information is derived from a foreign government must be concealed. Documents containing FGI shall keep the FGI segregated from U.S. classified portions. Release or disclosure of FGI back to the source country is not implied and must be approved by the responsible agency. Documents containing FGI from more than one country and/or international organization shall keep the FGI from each individual country or international organization segregated in separate portions. The release or disclosure of FGI to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation. (See the ISOO Directive 32 CFR 2001.23D-E and the CAPCO Implementation Manual for marking guidance.) Unclassified FGI is withheld from public release until approved for release by the source country.

2-6. FOCAL POINT INFORMATION. Focal Point Information is a Joint Chiefs of Staff program. The system uses unique code words to Protect Operationally Sensitive Information and alert responsible personnel to deliver the traffic to specifically authorized personnel only. Each Focal Point Program has its own Security Classification Guide that has been specifically written to provide unique guidance on handling, storage and disclosure of the information. CCR 380-14 is not the final authority for ACCM information; personnel needing access to or having questions concerning Focal Point should contact CCJ3 for indoctrination.

2-7. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI). The USCENTCOM SSO is responsible for indoctrination of personnel in CNWDI. These personnel must have a need to know, verified by an O-6 or above and have a final SECRET or TOP SECRET clearance.

2-8. OPERATIONS SECURITY (OPSEC) INFORMATION. OPSEC is governed by USCENTCOM Regulation (CCR) 530-1, Operations Security; Joint Pub (JP) 3-13.3, Joint Doctrine for Operations Security and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3213.01C; Joint Operations Security. CCJ3 is the CENTCOM OPR for OPSEC. OPSEC is the process of identifying and analyzing critical information pertinent to the military operation or activity and executing measures to eliminate or reduce vulnerabilities to a manageable level. OPSEC indicators result from friendly detectable actions or from open-source information. OPSEC generally is NOT classified but is a program designed to minimize indicators.

2-9. JOPES TPFDD INFORMATION. The Joint Operations Planning and Execution System (JOPES) is designated as SECRET.

a. Access to JOPES is limited to authorized U.S. personnel only possessing a FINAL SECRET clearance. Access to JOPES by coalition personnel is not authorized. The release of certain JOPES TPFDD information is permitted as approved by CCJ3 and coordinated with CCJ3-S and the command foreign disclosure office (CCJ2-FDO).

b. Release of JOPES force movement information must be coordinated with CCJ3-S, the OPR for JOPES at USCENTCOM as well as CCJ2-FDO.

c. Although individual data elements by themselves may not be classified, the data in aggregation could portray the scope of operations, force deployments, location centers, etc.

d. JOPES information is SECRET but certain data elements may be declassified for purposes of transportation planning upon execution; the data elements which may be declassified are limited to those data elements specifically required to schedule airlift, sealift, or ground movement as appropriate.

e. JOPES classification guidance is governed by existing CJCSI 3122 Series, JOPES Volumes I-III and applies to all Contingency Planning, Crisis Action Planning, and Exercise TPFDDs supporting USCENTCOM

THIS PAGE INTENTIONALLY LEFT BLANK

.

# CHAPTER 3
# DISCLOSURE AND RELEASE OF INFORMATION

3-1. DISCLOSURE OF UNCLASSIFIED INFORMATION When certain details of information are unclassified, it does not authorize automatic public disclosure. . Information must be reviewed for security concerns and approved in accordance with DOD Instruction (DODI) 5230.29, Security and Policy review of DOD information for Public Release and the Commander's OPSEC Critical Information List (CIL). USCENTCOM Review procedures must also specifically address the identification of For Official Use Only (FOUO). PA officers that review information for web posting must use OPSEC as a guide prior to posting information, photographs, or videos on websites readily accessible to the public. Direct proposed disclosures of unclassified information through the USCENTCOM Public Affairs Office (CCCI), Command OPSEC Program Manager (CCJ3-IO OPSEC), and/or the Command Records Branch (CCJ6-RD), as appropriate. The term "disclosure" includes, but is not limited to, any technical data, articles, speeches, photographs, brochures, advertisements, presentations, displays or websites.

3-2. DISCLOSURE OF CLASSIFIED INFORMATION. DOD considers disclosure as "The sharing of classified information, through oral, visual, or documentary means."

a. Disclosure 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 in accordance with DOD 5200.1-R and USCENTCOM Regulation (CCR) 380-1. It is the responsibility of the individual disclosing the information to verify the recipient's appropriate security clearance, this replaces 'need to know' and is known as 'responsibility to provide'.

b. Disclosure to Foreign Partners. Classified information released to foreign nationals, foreign governments, or international organizations must be IAW the National Disclosure Policy and USCENTCOM Regulation 380-5, Disclosure of U.S. Classified Military Information to Foreign Governments and International Organizations. All disclosures of classified military information will be coordinated through the Command Foreign Disclosure Office (CCJ2-FDO), the appropriate Director/Chief of Special Staff, and their designated Foreign Disclosure Representative.

3-3. RELEASE OF CLASSIFIED INFORMATION. Release is "the physical transfer of classified information that an originator has predetermined to be releasable or has been released, through established foreign disclosure procedures and channels, to the foreign country(ies)/international organization(s) indicated."

3-4. WRITING FOR RELEASE. USCENTCOM works closely with coalition partner nations. Appropriate risk management is necessary to ensure the success of missions USCENTCOM conducts with other nations. Originally produced USCENTCOM products will, to the maximum extent allowable by Executive Order and DOD directives, be marked to facilitate information sharing among coalition partners. See Chapter 6-45, Additional Markings, for information on caveat limitations. Under no circumstances will anyone remark or regrade information from

other government agencies. The FDO is the designated office for coordinating release of other agencies' information to foreign partners and/or international organizations.

3-5. LIMITATIONS ON RELEASE. The following information may not be released or authorized for release:

a. Classified information on the recipient country or its territories, with certain exceptions contained in Director of Central Intelligence Directive (DCID) 6/7.

b. Classified information which would:

(1) Jeopardize current or future intelligence sources or methods.

(2) Jeopardize existing or planned intelligence activity, or the safety, welfare, or reputation of individuals connected therewith.

(3) Be used to damage U.S. relations with friendly or allied countries.

(4) Be used for propaganda purposes.

(5) Jeopardize counterintelligence operations.

(6) Reasonably be expected to be acquired by hostile countries.

c. Classified information obtained from another government without its consent.

d. Classified information that could be harmful or prejudicial to the national security, foreign policy, or intelligence interests of the U.S.

e. Classified information, the release of which would be contrary to U.S. federal legislation or to agreements or treaties between the U.S. and foreign nations.

f. Classified information, not publicly available, on a U.S. person, unless authorized by EO 13526.

# CHAPTER 4
# ORIGINAL CLASSIFICATION AUTHORITY

4-1. DESCRIPTION. Original classification is the initial decision that information produced by USCENTCOM could be expected to cause damage to national security if subjected to unauthorized disclosure, and the interests of national security are best served by applying the safeguards of EO 13526 to protect it. This decision may be made only by persons who have been specifically delegated the authority to do so and have received training in the exercise of this authority. The training must be documented and maintained in the Security Manager Book located with the USCENTCOM SSO.

4-2. POLICY. IAW Secretary of Defense (SecDef) Memorandum, 13 November 95, Delegation of Original Classification Authority, the Commander, USCENTCOM (CDR), Deputy Commander (DCDR) and USCENTCOM Chief of Staff (COS) are delegated Top Secret OCA IAW EO 13526.

4-3. DELEGATION OF AUTHORITY. The Under Secretary of Defense for Intelligence, USD(I) is the delegation authority for SECRET OCA for USCENTCOM. This authority may not be further delegated.

4-4. TRAINING. Persons who have been delegated original classification authority must receive a briefing and training annually on their duties as an OCA from the SSO.

4-5. PROCESS. Original classification decisions made by USCENTCOM OCAs are limited to information produced by or for USCENTCOM or its activities. When making a decision to classify information, the designated USCENTCOM original classification authority shall personally review the information to:

a. Determine that the information is owned by, produced by, produced for, or is under the control of USCENTCOM.

b. IAW EO 13526, determine that the information falls within one or more of the categories of information listed below:

(1) Military plans, weapon 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 U.S., including confidential sources.

(5) Scientific, technological, or economic matters relating to national security.

(6) U.S. Government programs for safeguarding nuclear materials or facilities.

(7) Vulnerabilities or capabilities of systems, installations, projects or plans relating to national security.

c. Determine that, if classification is applied or reapplied, there is a reasonable possibility that the information can be provided protection from unauthorized disclosure.

d. Determine that the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security of the U.S., and that the damage can be identified or described. NOTE: USCENTCOM regularly must justify (identify or describe) why documents have been classified. SSO and ISB will assist OCAs in preparing the justification.

e. Determine which level of classification is to be applied.

(1) Apply TOP SECRET classification to information when its unauthorized disclosure is expected to cause exceptionally grave damage to national security the original classification authority personally is able to identify or describe. Only the Commander, Deputy Commander or COS can make the decision to classify USCENTCOM information as TOP SECRET.

(2) Apply SECRET to information for which the unauthorized disclosure expected to cause serious damage to national security that the original classification authority is personally able to identify or describe. The decision to classify USCENTCOM information SECRET can be made only by those officials designated in paragraph 4-3 of this regulation and only in those areas of expertise for the OCA.

(3) Apply CONFIDENTIAL to information for which the unauthorized disclosure reasonably could be expected to cause damage to the national security that the original classification authority is personally able to identify or describe. The decision to classify USCENTCOM information CONFIDENTIAL may be made only by those officials designated in paragraph 4-3 of this regulation and only in those areas of expertise for the OCA.

f. Ensure the document is marked properly (see Chapter 6)and includes the classification authority block on the face (first page) of each document or other media to indicate the name of the person and office symbol who classified the document; the authority (if classified by an OCA, after "Reason" list the section of an Executive Order or if derivatively classified, after "Derived from" list the classification guide title, number and date or if from source, the originating agency, serial number and date of the classified source product) for the classification determination, and after the declassification instructions:

(1) CLASSIFIED BY: the identification by name or personal identifier and position title of the OCA, the agency, and the office of origin

(2) CLASSIFICATION REASON: the concise reason for classification that, at a minimum, cites one of the classification categories listed in Section 1.4 of E.O. 13526

(3) DECLASSIFY ON: the duration of the original classification decision, specified as the date or event that corresponds to the lapse of the information's national security sensitivity. Valid declassification values include (a) a date of no more than 25 years from the original classification decision or the information's origin. The following format must be used: YYYMMDD; (ban event. Events must be reasonably definite and foreseeable; (c) an exemption category of 50X1-HUM or 50X2-WMD or am ISOO-approved designator reflecting the ISCAP approval for classification beyond 50 years. The "50X1-HUM" marking is used when the information clearly and demonstrably could reveal a confidential human source or a human intelligence source. With the implementation of E.O. 13526, and for the purposes of reusing or creating new classified documents, "50X1-HUM" replaces "25X1-human" which is no longer an authorized declassification instruction. "25X1-human" must be removed from all automated marking systems. As stated in section 1.5(d) of E.O. 13526, no information may remain classified indefinitely; therefore, information marked as "25X1-human" will be subject to automatic declassification. Since the "25X1-human" marking will continue to be found on originally and derivatively classified documents for many years, it will be treated as having the same classification duration as "50X1-HUM," and that information is not subject to automatic declassification for up to 75 years.* The "50X2-WMD" marked is used when the information clearly and demonstrably could reveal key design concepts of weapons of mass destruction; (d) 25X1, EO 12951 (Note: Per DNI Memo E/S 00400, dated 26 May 2010, value replaces the "DCI Only: and "DNI Only" markings.) The DNI prescribed the "25X1, EO 12951" marking for use on information described in EO 12951, Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems and previously marked with DNI Only or DCI Only; (e) An exemption category of 25X, date or event " (where "#" is a number from 1 to 9) ; (f) An exemption category of 50X, date or event " (where "#" is a number from 1 to 9); and (g) An exemption category of 75X, date or event " (where "#" is a number from 1 to 9). [Approved exemption codes are in ISOO Implementing Directive (32 CFR Parts 2001 and 2003).].

(4) Date of origin of the document

4-6. IMPROPERLY CLASSIFIED USCENTCOM DOCUMENTS. Due to the sheer volume of information and documents that USCENTCOM produces, documents will at times be improperly marked or classified. During FOIA requests or during court proceedings documents could be requested that an OCA must first do a determination of classification. When determining a document warrants classification, an OCA will issue a memorandum that properly classifies (or declassifies) the document(s). See Figure 4-1.

4-7. PROHIBITIONS. Anyone who fraudulently applies the name of an OCA as the classification authority to a document the OCA did not personally review and approve is subject to administrative sanctions such as loss of access or suspension of clearance.

UNITED STATES CENTRAL COMMAND
7115 SOUTH BOUNDARY BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5101

CCJ2 3 NOV 05

MEMORANDUM FOR Commander, USCENTCOM

SUBJECT: Classification of Document: NAME or DESCRIBE document. (U)

1. (U) Pursuant to Executive Order 12958 and IAW Central Command Regulation 380-1, I have been designated an original classification authority for documents classified by HQUSCENTCOM and subordinate units.

2. (U) I have reviewed the appended document and find the documents are classified SECRET REL USA due to reasons 1.4 (a) and (b) of EO 12958.

3. (U) POC is .

OCA NAME
MG, USA
Director of ?????

Figure 4-1
Classification Memorandum

# CHAPTER 5
# DERIVATIVE CLASSIFICATION

5-1. DESCRIPTION. Most classified documents produced within USCENTCOM are the result of derivative classification. Derivative classification is the act of incorporating, paraphrasing, restating, or generating in a new form any formation that is already determined to be classified by an OCA in a source document, classification guide, or other OCA guidance document. The application of classification markings and declassification instructions to a document or other material as directed by a security classification guide, security classification memorandum, a source document, or other source material is derivative classification. Under no circumstances will such information be cited as originally classified by an USCENTCOM classification authority.

5-2. POLICY. USCENTCOM regulation 380-14 is the Security Classification Guide (SCG). Any products derived from other agency documents will list that agency's document or in the use of more than one document, an addendum will accompany the USCENTCOM product listing ALL products used and their classification. Activity security managers will ensure all personnel derivatively classifying documents have been properly trained.

5-3. INDIVIDUAL RESPONSIBILITY. All persons performing derivative classification will:

a. Observe and respect the original classification decision unless superseded by OCA guidance, and carry forward to any newly created document the pertinent classification markings from the source document(s), classification guide(s), or other applicable OCA guidance. Do not 'downgrade' the information to ensure releaseability. Personnel will refer any requests to regrade the material to the originating agency or individual.

b. Apply classification markings, declassification instructions, warning messages, or other means of identification to the derivatively classified material (see Chapter 6). When derivatively classifying from more than one classified source, use the highest level of classification and all the caveats in accordance with the CAPCO guide on the top and bottom of the document or other media in order to afford the information the greatest degree of protection; include all the warning messages from among the sources on the face (first page) of the document or media.

c. Use only authorized sources of instructions about the classification of the information in question. Authorized sources of instructions about classification are security classification guides, other forms of classification guidance, and markings on material from which the information is extracted.

d. Include a list of all documents or sources used in the derivative classification appended to the last page.

e. Ensure the document is marked properly (see Chapter 6) and includes the date of origin and the classification authority block on the face (first page) of each document or other media to indicate the name of the person and office symbol who derivatively classified the document; the authority (after "Derived from" list the classification guide and date or the serial and the agency,

serial number and date of the classified source product) for the classification determination, and after the declassification instructions:

(1) CLASSIFIED BY: the identification by name and office symbol of the derivative classifier

(2) (U) DERIVED FROM:

(If the information classified under the classification guide is the only classified information contained in a document), Classification guide title and number, date published. For example,
DERIVED FROM: USCENTCOM Security Classification Guide, CCR380-14; date published
or
(If derived from one classified source or classification guide) Agency, serial number, date of classified source. For example,
DERIVED FROM: DIA, 12123434-11, 31 October 2011
or
(If derived from more than one source) Multiple Sources. For example,
DERIVED FROM: Multiple Sources

The author must include all the sources, including the classification in the list of sources.
If the classification document is an analytical intelligence product that will be disseminated, all the sources must be formatted as endnotes in accordance with ICD 206.
If the classification document is an analytical intelligence product that will be disseminated, in accordance with ICD 206, the endnote format for citing this classification guide will be [Endnote number] (U//FOUO) USCENTCOM; CCR380-14; date published; USCENTCOM Security Classification Guide CCR380-14 (U//FOUO); page number; overall classification is U//FOUO; CCR 380-14 is the USCENTCOM Classification Guide that provides guidance on classifying intelligence data; according to it, the referenced data should be classified list the classification.

(3) DECLASSIFY ON: the duration of the original classification decision, specified as the date or event that corresponds to the lapse of the information's national security sensitivity carried forward from the source document's "Declassify On" line or from the applicable classification guide. Valid declassification values include: (a) a date up to 25 years from the original classification decision; (b) a specific event within 25 years; (c) an exemption category of 50X1-HUM or 50X2-WMD or am ISOO-approved designator reflecting the ISCAP approval for classification beyond 50 years; (d) 25X1, EO 12951 (prescribed by the DNI for use on information described in EO 12951, Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems and previously marked with DNI Only or DCI Only); (e) 25X1-human (per ISOO, this marking is to be carried over by the derivative classifier until the originator has authorized the use of the 50X1-HUM marking; (f) 25X1 to 25X9, with a date or event; (g) See approved exemption codes in ISOO Implementing Directive (32 CFR Parts 2001 and 2003).]; and (h) Absent guidance from an OCA with jurisdiction over the information, a calculated 25-year date from the date of the source information. When the source date cannot be readily determined, calculate a date 25 years from the current date.

(4) Date of origin of the document

Example Declassification Blocks:

a. ORIGINAL CLASSIFICATION BLOCK:

Classified By: John E. Doe, Chief Division 5
Reason: 1.4(a)
Declassify On: 20151231

b. DERIVITIVE CLASSIFICATION BLOCK:

Classified By: Joe Carver, Director
Derived From: Department of Good Works Memorandum dated June 27, 2010, Subj: (U) Examples
Declassify On: 20151231

5-4. OTHER CLASSIFICATION GUIDES. USCENTCOM, as a combatant command, has mission responsibility for a geographic area designated by the President. Services (U.S. Army, Navy, Air Force and Marines) are force providers. Certain systems fielded by the Services have published classification guides. In those instances where declassification or classification determinations are requested, each security guide will be used as it relates to the USCENTCOM mission, area of responsibility (AOR) and the platform (sensors, capabilities, etc.) that are Service responsibilities.

THIS PAGE INTENTIONALLY LEFT BLANK

# CHAPTER 6
# MARKING CLASSIFIED INFORMATION

6-1. OVERALL CLASSIFICATION. See Figure 6-1. Every classified document must be marked to show the highest classification of information it contains. This marking must be conspicuous enough to alert anyone handling the document that it is classified. The overall classification will be marked, stamped, or affixed (with a sticker, tape, etc.) in letters larger than the rest of the text on:

a. The front cover, if there is one.

b. The title page, if there is one.

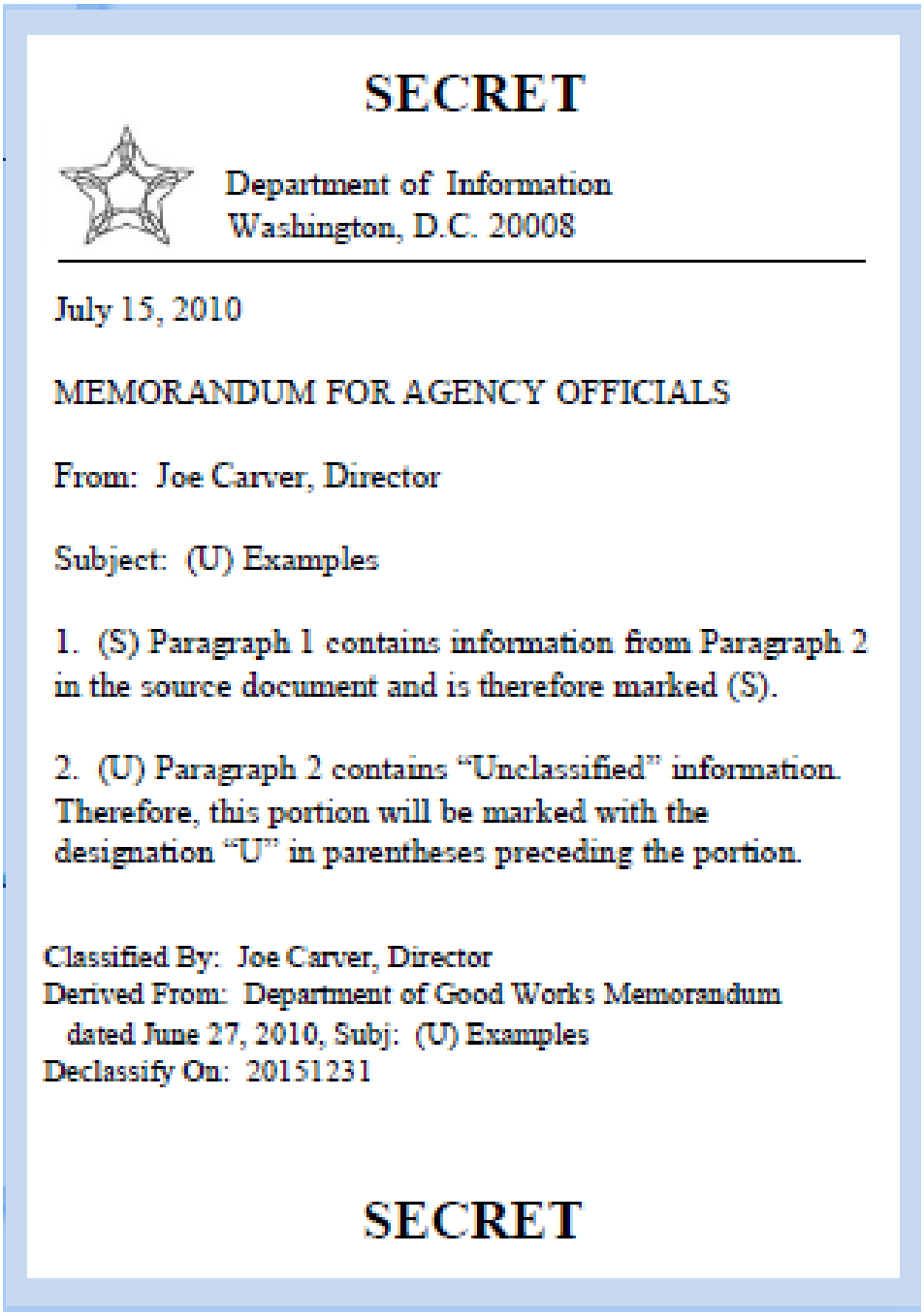
c. The first page. If the document has no front cover, the first page will be the front page. If it has a cover, the first page is defined as the first page you see when you open the cover. In some documents, the title page and first page may be the same.

d. The outside of the back cover, if there is one.

6-2. SOURCE OF CLASSIFICATION. Every USCENTCOM document will include the directorate and branch that produced the document within the classification line.

a. ORIGINAL CLASSIFICATION. Every originally classified document must have a "Classified by" line placed on the face of the document that identifies the original classification authority responsible for classification of the information it contains. The original classification authority shall be identified by name or personal identifier and position title. Application of this identifying data indicates the OCA personally reviewed the document and rendered a classification decision. See Section 4.

b. DERIVATIVE CLASSIFICATION. Persons who apply derivative classification markings shall be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action. (32CFR, Part 2001). The first page of a derivatively derived document will be marked with a "Classified by" line, "Derived from" line, and a "declassify on" line (See Section 5 and Figure 6-1). Each source document with DERIVED FROM: Multiple Sources in the classification authority block, must include a list of all documents or sources used in the derivative classification appended to the last page per E.O. 13526, Section 1.6 and 2.1; ISOO Implementing Directive (32 CFR Parts 2001 and 2003), the CAPCO Implementation Manual, or inserted as endnotes per ICD 206.



SECRET

Department of Information
Washington, D.C. 20008

July 15, 2010

MEMORANDUM FOR AGENCY OFFICIALS

From: Joe Carver, Director

Subject: (U) Examples

1. (S) Paragraph 1 contains information from Paragraph 2 in the source document and is therefore marked (S).

2. (U) Paragraph 2 contains "Unclassified" information. Therefore, this portion will be marked with the designation "U" in parentheses preceding the portion.

Classified By: Joe Carver, Director
Derived From: Department of Good Works Memorandum dated June 27, 2010, Subj: (U) Examples
Declassify On: 20151231

SECRET

Figure 6-1
Derivative Classification Example

6-3. DECLASSIFICATION INSTRUCTIONS. Every classified document must be marked on the face of the document with a "Declassify on" line, with instructions concerning the declassification of the information in the document. For originally classified USCENTCOM documents, the OCA will choose the date of declassification not to exceed 25 years from date of origination. When a document or item of material is marked for downgrading or declassification on a date or event, the holder shall, prior to downgrading, declassification, or removal of

classification markings, confirm that the OCA(s) for the information has not extended the classification period. This can be done by reference to a security classification or declassification guide or to other appropriate guidance issued by the OCA or by consultation with the OCA. For derivative documents, use the latest date of declassification of the documents. Refer to E.O. 13526, Section 1.6 and 2.1; ISOO Implementing Directive (32 CFR Parts 2001 and 2003); the CAPCO Implementation Manual; and DoD 5200.1-R for additional instructions.

6-4. MARKING IN THE ELECTRONIC ENVIRONMENT. General Guidance. Where special provisions for marking some types of computer-generated information are needed, the requirement remains to identify as clearly as possible the information that requires protection and the level of protection it requires, and to make available either on the item or by other means, the other required information.

a. Classified information resident in an electronic environment is subject to all of the requirements of Reference (d) and shall be:

b. Marked with the required classification markings to the extent that such markings are practical, including banner line with overall classification and control markings, portion markings, and classification authority block.

c. Marked with the required classification markings when appearing in or as part of an electronic output (e.g. database query) so that users of the information will be alerted to the classification status of the information.

d. Marked in accordance with derivative classification procedures (see paragraph 8.c of this enclosure), maintaining traceability of classification decisions to the OCA. In cases where classified information in an electronic environment cannot be marked in this manner, a warning shall be applied to alert users that the information may NOT be used as a source for derivative classification and providing a point of contact and instructions on how to obtain further guidance on use and classification of the information.

e. Prohibited from use as source of derivative classification if the information is dynamic in nature (e.g. wikis and blogs) and is not marked as required by References (d) and (e) and this Volume.

(1) All e-mail, blog and wiki entries, bulletin board posting, and other electronic messages shall be marked as finished documents, in accordance with the requirements of this section, due to the originator's inability to control retention and redistribution once transmitted. They shall not be marked as working papers.

(2) Some organizations use automated tools to mark electronic messages (e.g., organizational messages, e-mails, and text or instant messages). It remains the individual's responsibility to properly mark classified messages, including banner marking, portion markings, and classification authority block when an automated tool is used.

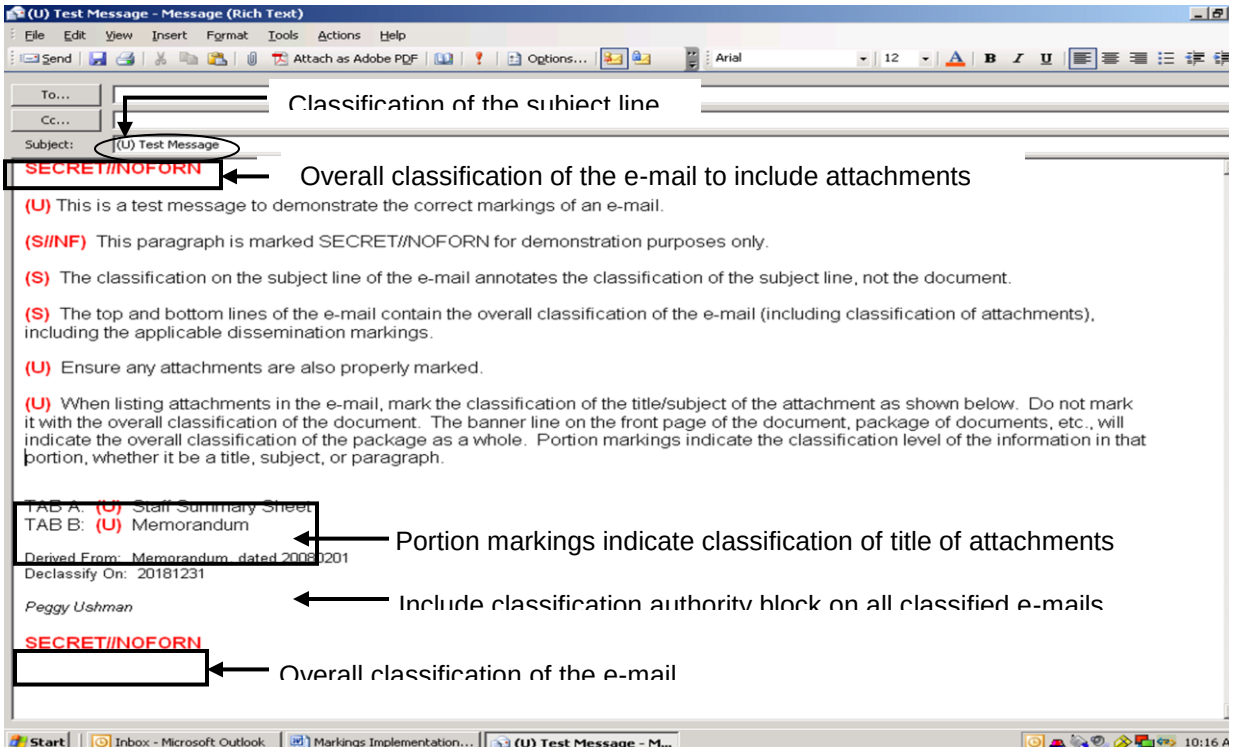
(3) Where fan-folded printouts are still used, classification markings on interior pages may be applied by the information system or equipment even though the markings may not meet the normal test of being conspicuous. Dissemination control markings and the classification authority block shall either be marked on the face of the document or be placed on a separate sheet of paper attached to the front of the document. Segments of such printouts removed for separate use or maintenance shall be marked as individual documents.

f. E-Mail Messages.

(1) E-mail transmitted on or prepared for transmission on classified systems or networks shall display the banner line at the top and bottom of the body of each message. A single linear text string showing the overall classification, to include dissemination and control markings, shall be included as the first line of text and at the end of the body of the message after the signature block (see Figure 16).

(2) The banner marking for the e-mail shall reflect the classification of the header and body of the message. This includes the subject line, the text of the e-mail, any classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail.

(3) Classified e-mail shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A text portion containing a uniform resource locator (URL) or reference (i.e., link) to another document shall be portion marked based on the classification of the content of the URL or link text, not the content to which it points. This is true even when the data accessible via the URL or link reflects a higher classification marking.



(4) The subject line's portion marking will show the classification of the subject line itself, not the overall classification of the e-mail. The subject line portion marking shall reflect the sensitivity of the subject alone and shall not consider the sensitivity of the e-mail content or attachments. Subject lines and titles may be portion marked before or after the subject or title.

(5) The classification authority block shall be placed after the signature block, but before the final banner line at the end of the e-mail. The block may optionally appear as a single linear text string instead of the traditional three line format.

(6) When forwarding or replying to an e-mail, individuals shall ensure that the markings used reflect the classification markings for all the content present in the resulting message and any attachments. This will include any newly drafted material, material received from previous senders, and any attachments.

(7) For unclassified e-mails or other messages transmitted over a classified system, the designation "UNCLASSIFIED" shall be conspicuously placed within the banner line and any dissemination controls, such as "FOUO" or "PROPIN" (Proprietary Information), that may apply must be included.

(8) E-mails used as transmittal documents shall be marked as required by ISOO Implementing Directive (32 CFR Parts 2001 and 2003). Place the instruction indicating the e-mail's overall classification level when separated from its enclosures just above the final banner line.

6-5. ADDITIONAL MARKINGS. USCENTCOM works in a joint, multi-national and coalition environment; therefore, information sharing is paramount for successful mission accomplishment. Additional markings that limit the ability to share information should be used sparingly on USCENTCOM documents and there should be no default classification. The following is not an all-inclusive list of additional markings but include special instructions for USCENTCOM personnel.

a. Not Releasable to Foreign Nationals (NOFORN). NOFORN is an intelligence dissemination caveat and governed by the Director of National Intelligence (DNI); the National Security Act of 1947, Section 103 (c)(5); DCID 6/6, Section IX.E; DCID 6/7; and National Disclosure Policy (NDP)-1. NOFORN indicates that this classified intelligence information may not be released in any form to foreign government, foreign nationals, foreign organizations, or non-U.S. citizens without the permission of the originator and in accordance with the provisions of DCID 6/7 and NDP-1. If the information did not come from an intelligence system or report, it will not be considered as NOFORN. Sections desiring to limit information to U.S. personnel only should use REL TO USA after the classification (i.e. S//REL TO USA). When a document or media contains both NOFORN and REL TO or NOFORN and EYES ONLY portions, NOFORN takes precedence for the markings in the top and bottom of the document or media. When a document or media contains both REL TO and uncaveated portions, NOFORN takes precedence in the classification markings in the top and bottom of the document or media. When all portions in a document or media are marked with REL TO and there is no common country,

NOFORN takes precedence in the classification markings in the top and bottom of the document or media. (See CAPCO Implementation Manual.)

b. Releasable To (REL TO). USCENTCOM shares information with several different organizations and affiliations. Derivative information that is not marked for release to coalition or multi-national organizations cannot be released. The USCENTCOM Foreign Disclosure Office (FDO) is responsible for approving Classified Military Information (CMI) for disclosure or release to a foreign government or international organization. The FDO requests originating agencies' approval for release of CMI to our coalition partners. Use REL TO followed by the country trigraph codes (listed in alphabetical order after USA) to list the countries authorized to receive the information. USA should always be the first country trigraph listed after the words "REL TO" in U.S. documents or media; after USA, ISO 3166 country trigraph codes shall be listed in alphabetical order followed by tetragraphic codes listed in alphabetical order; each code is separated by a comma and a space. Authorized trigraphs for countries are listed in ISO 3166. Authorized tetragraphs are listed in the CAPCO APPENDIX A, Tetragraph Table. USCENTCOM uses the GCTF tetragraph instead of listing out each country for coalition members assigned to USCENTCOM as well as when appropriate for sharing in support of OEF or other terrorism related needs. The FDO, SSO and CSB are available to answer any marking questions you may have.

c. FOREIGN GOVERNMENT INFORMATION (FGI). The FGI marking is used in U.S. products to denote the presence of foreign-owned or foreign-produced information. These markings are used based on sharing agreements or arrangements with the source country or international organization (See E.O. 13526, Section 6.1(r); and ISOO Directive 32 CFR Parts 2001 and 2003.). USCENTCOM agrees to protect the information at the equivalent level of classification of the information in the U.S. system of marking. FGI material usually comes with limiting instructions and must be followed to preserve U.S. relationships and information sharing. ISO 3166 country trigraph codes shall be listed in alphabetical order followed by tetragraphic codes listed in alphabetical order; each code is separated by a space. Authorized trigraphs for countries are listed in ISO 3166; authorized tetragraphs are listed in the CAPCO APPENDIX A, Tetragraph Table. Documents with contain FGI data and U.S> data must keep the FGI portions separate from the U.S> portions. See the CAPCO Implementation manual for marking guidance.

d. NATO DOCUMENTS. NATO documents should be marked in accordance with U.S. Security Authority for NATO (USSAN) Instruction 1-69 and USSAN 1-07. Just because USCENTCOM personnel possess a valid U.S. clearance does not mean they have been indoctrinated for NATO material.

e. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM). ACCM, sometimes referred to as Special Category or SPECAT, handling caveats appear on sensitive, classified military information. Personnel receiving information with ACCM handling instructions are limited to those with a need to know. Specifically designated offices handle indoctrination into the appropriate ACCM.

# CHAPTER 7
# DECLASSIFICATION AND DOWNGRADING

7-1. DESCRIPTION. Declassification and regrading is the process of changing the classification of USCENTCOM information. USCENTCOM processes Automatic, Systematic and Mandatory reviews of classified material. Automatic reviews are classified records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code; Systematic reviews are of permanently historical value excepted from automatic declassification under section 3.3 of EO 13526 and that the Archivist of the US has deemed of permanent historical value. Mandatory review is performed in response to a reasonable request for a review describing the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort.

7-2. POLICY. Information meeting the classification requirements of this guide shall remain classified as long as required for national security. EO 13526, 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.

7-3. (U) DECLASSIFICATION/EXEMPTION. The "DECLASSIFY ON" column specifies the date or event for declassification or the 25-year automatic declassification exemption category as described in E.O. 13526, Section 1.6 and 2.1; ISOO Implementing Directive (32 CFR Parts 2001 and 2003); the CAPCO Implementation Manual; and DOD 5200.1-R. When deciding how to complete the “DECLASSIFY ON” line, an original classification authority will have the following choices:

a. (U) A date of no more than 25 years from the original classification decision or the information's origin. The following format must be used: YYYYMMDD.

b. (U) An event. Events must be reasonably definite and foreseeable.

c. (U) “50X1-HUM” marking used when the information clearly and demonstrably could reveal a confidential human source or a human intelligence source.

d. (U) “50X2-WMD” marking used when the information clearly and demonstrably could reveal key design concepts of weapons of mass destruction.

e. (U) Per ISOO Notice 2012-02: This marking is no longer authorized. “25X1, EO 12951” (Note: Per DNI Memo E/S 00400, dated 26 May 2010, value replaces the “DCI Only” and “DNI Only” markings).

f. (U) An exemption category of "25X#, date or event" (where "#" is a number from 1-9). (The use of exemptions from automatic declassification by agencies must be authorized in accordance with ISOO Implementing Directive, § 2001.26.)

g. (U) An exemption category of "50X#, date or event" (where "#" is a number from 1-9). (The use of exemptions from automatic declassification by agencies must be authorized in accordance with ISOO Implementing Directive, § 2001.26.)

h. (U) An exemption category of "75X#, date or event" (where "#" is number from 1-9). (The use of exemptions from automatic declassification by agencies must be authorized in accordance with ISOO Implementing Directive, § 2001.26.)

7-4. DOWNGRADING. Downgrading is the change from a higher security classification to a lower level due to the information or means of collecting the information not meeting the prerequisites of EO 13526.

a. Instructions. Cancel (i.e., line through) old classification markings and substitute the new ones when a document is downgraded according to its markings. At a minimum, the markings on the cover (if one exists), title page (if one exists), and the first page shall be changed. If information no longer meets the requirements for classification at a higher level but still needs protecting, downgrading instructions will be included. For example, a TOP SECRET plan can be marked, 'DOWNGRADE to SECRET after execution.' The marking should be on the front page and be similar to the following:

CLASSIFIED BY: Joe Snuffy
DERIVED FROM: USCENTCOM SCG 0707
DECLASSIFY ON: 15 July 2017
DOWNGRADE to CONFIDENTIAL following mission completion

b. Authority to Downgrade. Information may be declassified and downgraded by those officials who have been delegated Original Classification Authority in this regulation and officials who have been delegated, in writing, declassification authority. The authority to declassify information extends only to information for which the specific official has classification, program, or functional responsibility. The CCJ6-RD Command Records Manager has designated the CCJ6-RDD, Chief, Declassification Management Section the authority to declassify or withhold records under the Automatic Declassification Program. Original Classification authorities may designate, in writing, members of their staffs in grades O5 and above to exercise declassification authority over information under their jurisdiction. A copy of delegation of declassification authority will be maintained by the security manager. An information copy will be forwarded to CCJ2-CSB. OCAs must ensure those personnel they designate as declassification authorities are trained, knowledgeable, and capable of making sound declassification decisions in regard to the specific information. The responsibility for the declassification decisions rests with the OCA, therefore coordination and oversight is imperative. Information not originally produced by USCENTCOM will not be regraded without the express consent of the ORIGINATOR of the information.

7-5. DOWNGRADING OR DECLASSIFICATION EARLIER THAN SCHEDULED. If a document is downgraded or declassified earlier than indicated by its markings, the guidance in paragraph 7-4, as appropriate, of this enclosure must be followed. In addition, place this information on the document:

a. The date of the downgrading or declassification re-marking.

b. The authority for the action (e.g., the identity of the OCA who directed the action or identification of the security classification guidance or instruction that required the action). When possible file a copy of the correspondence authorizing the early downgrading or declassification with the document.

c. Upgrading. If a document is upgraded, all classification markings affected by the upgrading shall be changed to the new markings. Also, place this information on the document:

(1) The date of the re-marking.

(2) The authority for the action (e.g., the identity of the OCA who directed the action, or identification of the correspondence or classification instruction that required it).

d. Extension of Classification. If information has been marked for declassification on a specific date or event and the duration of classification is subsequently extended, then:

(1) The "Declassify On:" line shall be changed to show the new declassification instructions.

(2) A notation shall be included on the front cover or first page indicating the identity of the OCA authorizing the extension or identification of the correspondence or classification instruction requiring it, and the date of the action.

e. Reclassification. Previously declassified information may be reclassified IAW ISOO Implementing Directive (32 CFR Parts 2001 and 2003). When reclassified, information shall be re-marked to clearly provide:

(1) New overall classification markings and portion markings to replace those that had been cancelled.

(2) A new classification authority block (i.e., identification of the OCA, reason for classification, and declassification instructions).

(3) The date the reclassification action was taken.

f. Bulk Changes. If the volume of material involved in a downgrading, upgrading, or declassification action is so large that individually re-marking each item may cause serious interference with operations, the custodian may attach a notice to the inside of the storage unit providing the information required by this section or section 11 of this enclosure, as applicable.

When individual documents are removed from the storage unit for use, they shall be marked in the manner prescribed. If documents are removed for transfer to another storage unit, they need not be re-marked if a proper notice is also posted to the new storage unit.

## CHAPTER 8
## PROPONENT

PROPONENT. The proponent of this regulation is the USCENTCOM Director of Intelligence, CCJ2, Special Security Office (SSO). Users can send comments and suggested improvements 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:

OFFICIAL:

KARL R. HORST
Major General, U.S. Army
Chief of Staff

WALTER L. CARTER JR.
LTC, U.S. Army
Deputy Chief, Resources and
Analysis Division, CCJ6-R

DISTRIBUTION: A (1 EA)

"SUMMARY OF CHANGES"

This regulation contains major revisions required by Executive Order (EO) 13526 dated 29 December 2009, Classified National Security Information, the Information Security Oversight Office (ISOO) Implementing Directive (32 CFR Parts 2001 and 2003), subsequent ISOO Notices, Intelligence Community Directive (ICD) 710 Classification and Control Markings System dated 11 September 2009, ICD 206 Sourcing Requirements for Disseminated Analytic Products dated 17 October 2007, ICD 208 Writing for Maximum Utility dated 17 December 2008, the Controlled Access Program Coordination Office's (CAPCO) Authorized Classification and Control Markings Register dated 31 May 2011, and the CAPCO Intelligence Community Classification and Control Markings Implementation Manual dated 31 May 2011. This revision combines information from CCR 380-1 with CCR 380-14; specifically chapters 2, 4-7. The entire regulation was restructured to provide a clearer understanding of the publishing function at all levels.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

| MANPOWER, PERSONNEL, AND ADMINISTRATION (CCJ1) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Daily personnel statistics | S | 1 month | 1.4(g) | Approximate numbers of deployed personnel may be released by the CCCI for official use |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

| INTELLIGENCE AND SECURITY (CCJ2/JICCENT) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. 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 |
| 2. Intelligence information obtained from CI/HUMINT | C | 10 years | 1.4(c) | If the source is not identified |
| 3. Intelligence exchange agreements | S | 10 years | 1.4(b) 1.4(c) | |
| 4. Products of analysis by USCENTCOM intelligence analysts | Refer to Table below | Refer to Table below | 1.4(c) | Refer to Table 1 below |
| Table 1. Classifying CCJ2 Analysis | | | | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 4.a. Assessment detail is equal to that of original source information and does not reveal intelligence sources or activities, or U.S. foreign relations activities, command plans or similar sensitive data, | 4.a.1. Assessment should be classified in line with original sources | Most restrictive declassification of all the declassifications of the original sources. | 1.4 (a)<br>1.4 (c)<br>1.4 (d)<br>1.4 (g) | |
| | 4.a.2. If all information in the assessment is derived only from sources marked S//REL TO USA, GBR and the assessment does not contain any original thoughts, the assessment is S//REL TO USA, GBR | Most restrictive declassification of all the declassifications of the original sources. | 1.4 (a)<br>1.4 (c)<br>1.4 (d)<br>1.4 (g) | |
| | 4.a.3. If all information in assessment is | Most restrictive declassification of all the declassifications of | 1.4 (a)<br>1.4 (c)<br>1.4 (d) | |

| | | | | |
|---|---|---|---|---|
| | derived from sources marked S//REL TO USA, GBR, but the assessments contains original thoughts and judgments, the assessment is S. | the original sources. | 1.4 (g) | |
| | 4.a.3. If assessment is derived from S//NF source and S//REL TO USA, GBR, and AUS source, assessment will be marked S//NF | Most restrictive declassification of all the declassifications of the original sources. | 1.4 (a)<br>1.4 (c)<br>1.4 (d)<br>1.4 (g) | |
| | 4.a.4. If assessment is derived from S//REL TO USA, GBR source, S//NF source and S//OC//NF source, assessment should be marked S//OC//NF | Most restrictive declassification of all the declassifications of the original sources. | 1.4 (a)<br>1.4 (c)<br>1.4 (d)<br>1.4 (g) | |
| | 4.a.5. If all information in an assessment or discussion is derived from UNCLASSIFIED sources, the analytic judgments or discussions that embody conclusions any intelligent observer could derive from publicly available information and that do not inherently reveal sensitive information about U.S. plans, policies or interests, the assessment should be marked | Not applicable | Not applicable | |

| | | | | |
|---|---|---|---|---|
| | UNCLASSIFIED. | | | |
| 4.b. Although all information in an assessment or discussion was derived from CLASSIFIED sources, if the analytic judgments or discussions that embody conclusions any intelligent observer could derive from publicly available information and that do not inherently reveal sensitive information about U.S. plans, policies or interests, | UNCLASSIFIED | Not applicable | | Not applicable |
| 4.c. Analytic judgments that depend on knowledge or understanding not available to the general public that originated from a sensitive source, to include<br><br>4.c.1. U.S. policymakers' priorities, interests or intentions should<br><br>4.c.2. U.S., allied or coalition partners' military operational plans, contingency plans, planning guidance, or | SECRET or TOP SECRET. See Note 1. | 25 years from the date of origination | 1.4 (a)<br>1.4 (c)<br>1.4 (d)<br>1.4 (g) | 4.c. Analytic judgments that depend on knowledge or understanding not available to the general public that originated from a sensitive source, to include<br><br>4.c.1. U.S. policymakers' priorities, interests or intentions should<br><br>4.c.2. U.S., allied or coalition partners' military operational plans, contingency plans, planning guidance, or contemplated future plans or guidance<br><br>4.c.3. Vulnerabilities of |

| | | | | |
|---|---|---|---|---|
| contemplated future plans or guidance<br><br>4.c.3. Vulnerabilities of the U.S. or foreign countries, their military forces, military systems, domestic infrastructure, political system, or other vital components | | | | the U.S. or foreign countries, their military forces, military systems, domestic infrastructure, political system, or other vital components |
| 4.d. Analytic judgments or products that provide an authoritative USCENTCOM position that draws on an understanding of classified information. | CONFIDENTIAL, SECRET or TOP SECRET. See Note 1. | 25 years from the date of origination | 1.4 (a)<br>1.4 (c)<br>1.4 (d)<br>1.4 (g) | Judgments that can be closely linked to specific classified sources should reflect the classification of those sources and should carry appropriate releaseability markings in accordance with ICD 710. Citing the authorities contained in this guide is not required as a basis for the classification of these judgments. |
| 4.e. Compilations of unclassified information, absent any analytic judgments, that in aggregate provide insight into national security or intelligence issues, beyond what would be obvious to an informed outside observer. | SECRET | 25 years from the date of origination | 1.4 (c) | Should carry appropriate releaseability markings in accordance with ICD 710. |
| 4.f. Analytic judgments that | SECRET | 25 years from the date of origination | 1.4 (c) | Should carry appropriate releaseability markings |

| | | | | |
|---|---|---|---|---|
| depend on analytic methodologies not available to the public. | | | | in accordance with ICD 710. |
| 4.g. Analytic judgments that depend on analytic methodologies not available to the public. | SECRET | 25 years from the date of origination | 1.4 (c) | Should carry appropriate releaseability markings in accordance with ICD 710. |
| 4.h. Analytic writings or discussions that provide insight into intelligence methods, gaps, or collection priorities but that do not include specific information derived from intelligence reports that would be covered by other derivative classification guidance. | SECRET | 25 years from the date of origination | 1.4 (c)<br>1.4 (d) | Should carry appropriate releaseability markings in accordance with ICD 710. |
| Information that reveals the existence of a USCENTCOM liaison relationship with a foreign intelligence service but that does not include specific intelligence information that would be covered by other derivative | SECRET | 25 years from the date of origination | 1.4 (c) | May be NOFORN or releasable to the foreign partner, as dictated by the terms of the applicable foreign exchange agreement. |

| | | | | |
|---|---|---|---|---|
| classification guidance. | | | | |
| 4.j. Assessment level of detail is different from original source information or it reveals intelligence sources or activities, U.S. foreign relations activities, command plans or similar sensitive data. | If original sources are S//OC/NF and S//NF, and assessment includes no OC references, assessment should be marked S//NF | Most restrictive declassification of all the declassifications of the original sources. | 1.4 (a)<br>1.4 (c)<br>1.4 (d)<br>1.4 (g) | |
| | If original sources are S//REL TO USA, GBR and assessment incorporates historical OC and NF data, assessment should be marked S//OC/NF | Most restrictive declassification of all the declassifications of the original sources. | 1.4 (a)<br>1.4 (c)<br>1.4 (d)<br>1.4 (g) | |

NOTE 1: Use the following definitions for deciding classification levels.
--- a. TOP SECRET shall be applied to information, when the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.
--- b. SECRET shall be applied to information when the unauthorized disclosure could reasonably be expected to cause serious damage to the national security that the OCA is able to identify or describe.
--- c. CONFIDENTIAL shall be applied to information when the unauthorized disclosure could reasonably be expected to cause damage to the national security that the OCA is able to identify or describe.

NOTE 2: Only the USCENTCOM Foreign Disclosure Office has the authority to approve the release of information to a non-U.S. entity. (i.e., Original sources were not marked REL TO but the analyst believes assessment could be made REL TO. The analyst must submit the data to the FDO who will determine if it can be released to specific foreign entities in accordance with National Disclosure Policy 1.).

APPENDIX C

| SECURITY (CCJ2-SSO) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Approved modifications to the requirements of DOD 5200.1-R during operations | C | Upon completion of operation | 1.4(g) | |
| 2. 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 |
| 3. Exploitable information or personnel security weaknesses in OCONUS areas | C | Upon correction, elimination of weakness, or 10 years, whichever is sooner | 1.4(g) | |
| 4. General security countermeasures | U | N/A | N/A | |
| 5. Loss of classified material | C | Upon regaining custody of material or following completion of damage assessment, whichever is later | 1.4(g) | |
| 6. 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) | |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D

| SOUTH EAST REGIONAL SERVICE CENTER (CCJ2/SE-RSC) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. ALE password | TS | Upon change | 1.4(a) | SCI |
| 2. COLISEUM password | TS | Upon change | 1.4(a) | SCI |
| 3. DAWN/HOCNET password | S | Upon change | 1.4(a) | |
| 4. GALE password | TS | Upon change | 1.4(a) | SCI |
| 5. JWICS LAN/WAN user ID | U | N/A | N/A | |
| 6. JWICS LAN/WAN password | TS | Upon change | 1.4(a) | SCI |
| 7. RMS password | TS | Upon change | 1.4(a) | SCI |
| 8. SAFE password | TS | Upon change | 1.4(a) | SCI |
| 9. Virus/network intrusions | S | Once neutralized | 1.4(g) | |
| 10. XDITDS password | TS | Upon change | 1.4(a) | SCI |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E

| COUNTERINTELLIGENCE / HUMAN INTELLIGENCE (CCJ2-X) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Requests for Procedures Special Investigative techniques IAW DoD 5240.1R | S | 10 years | 1.4(c) | Classified based on operational means |
| 2. Number and Category of CI/CE cases within AOR | C<br>S | 10 years | 1.4(c) | NOFORN |
| 3. CI Force Protection Vulnerability Assessments | U//FOUO<br>to<br>S | 0-25 years | 1.4(c) | Based on assessment of identified vulnerabilities and correction of identified problems |
| 4. Tasking which reveals impending U.S. intelligence operations, or U.S. intelligence targets or intelligence objectives | S//NOFORN | May be exempted : Declassify 10 to 25 years from date info is classified if reveals actual U.S. military war plans that remain in effect<br>Sensitive operations maybe classified higher or carry restricted assess if requested | 1.4(a)<br>1.4(c)<br>1.4(g) | Tasking and information in direct support of planned, impending or ongoing U.S. intelligence operations will not be shared without prior DCI or his designated agent's approval. |
| 5. Individual or comprehensive lists of foreign intelligence or operational targets | S//NOFORN<br>or<br>Higher | May be exempted : Declassify 10 to 25 years from date info is classified if the identity of a confidential source, or a human intelligence source, or information about the application of an intelligence source or method | 1.4(a)<br>1.4(b)<br>1.4(d)<br>1.4(g) | Target information in direct support of planned, impending, or ongoing U.S. military operations |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |

| | | | | |
|---|---|---|---|---|
| 6. Target lists that reveal impending U.S. intelligence operations or intelligence objectives | S//NOFORN<br>or<br>Higher | May be exempted : Declassify 10 to 25 years from date info is classified if the identity of a confidential source, or a human intelligence source, or information about the application of an intelligence source or method | 1.4(a)<br>1.4(b)<br>1.4(c)<br>1.4(d)<br>1.4(g) | Information is direct support of planned, impending, or ongoing U.S. intelligence operations will not be shared without prior DCI or his designated agent's approval |
| 7. CI Operational Concept (CIOC) or CI Special Operational Concept (CISOC). This includes CI-Specific CONOPS (i.e. JCIUs, etc.) | S//NOFORN | Declassify 10 years from date info is classified | 1.4(a)<br>1.4(c) | Any information about the purpose, subject or target, objectives, and methods will be classified |
| 8. Requests for Procedure 1-4 and 10-15, AR 381-10. | U | | 1.4(a) | Will be classified only if operational activities would be disclosed – classification will be based on the classification of the source material. |
| 9. Requests for Procedures 5-9, AR 381-10. | S | Declassify 10 years from date info is classified | 1.4(a) | Any information about the purpose, subject or target objectives, and methods will be classified. |
| 10. Relations between CENTCOM CI elements and other U.S. CI and investigative/intelligence agencies. | U or S | Declassify 10 years from date info is classified | 1.4(a) | UNCLASSIFIED if relationship is overt.<br>SECRET if relationship is covert. (Per DoDI C-5240.8) |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 11. Use of CI assets in foreign intelligence and special activities. | S | May be exempted: Declassify 10 to 25 years from date info is | 1.4(a)<br>1.4(b)<br>1.4(c) | Per DoDI C-5240.8 |

| | | | | |
|---|---|---|---|---|
| | | classified if information would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States | 1.4(d) | |
| 12. Information officially received from foreign agencies concerning personal security investigations. | C | Declassify 10 years from date info is classified | 1.4(b) | Protected as CONFIDENTIAL unless the foreign government authorizes it to be handled as UNCLASSIFIED. (Per DoDI C-5240.8) |
| 13. Spot Reports for non-investigative activity – i.e., threats against persons or property. | U to C | Declassify 10 years from date info is classified | 1.4(a) | CONFIDENTIAL if report would compromise a classified source. |
| 14. CI/CE Investigations | C to TS | May be exempted : Declassify 10 to 25 years from date info is classified if the identity of a confidential source, or a human intelligence source, or information about the application of an intelligence source or method | 1.4(a)<br>1.4(c)<br>1.4(d) | See AR 381-47 (S) for additional security classification guidance. Information may have caveats and require Special Access |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 15. Fact that USCENTCOM element is conducting a specific CI/CE investigation, project, | C to S | Declassify 10 years from date info is classified | 1.4(a)<br>1.4(c) | Minimum of Confidential. See NOTES 1, 2, and 3. |

| | | | | |
|---|---|---|---|---|
| operation, or other activity. | | | | |
| 16. Initial SAEDA report. | C to S | Declassify 10 years from date info is classified | 1.4(a)<br>1.4(c)<br>1.4(g) | All initial SAEDA reports will be classified a minimum of CONFIDENTIAL ; including the date/location of incident. See NOTE 2. |
| 17. Agent Reports and Investigative Memorandum for Record (IMFR). | C to S | Declassify 10 years from date info is classified | 1.4(a)<br>1.4(c)<br>1.4(d)<br>1.4(g) | Minimum of CONFIDENTIAL See NOTE 1 and 2. |
| 18. Identity of Subject(s) of investigation. | C to S | Declassify 10 years from date info is classified | 1.4(a)<br>1.4(c) | Minimum of CONFIDENTIAL. See Note 1 and 2. |
| 19. True name of CI/CE investigative source or other identifying personal data. | C | May be exempted : Declassify 10 to 25 years from date info is classified if the identity of a confidential source, or a human intelligence source, or information about the application of an intelligence source or method | 1.4(a)<br>1.4(c)<br>1.4(d)<br>1.4(g) | See NOTE 1. |
| 20. Case Control Number (CCN) or Nickname. | U | Declassify 10 years from date info is classified | 1.4(a) | When standing alone. Classify appropriately when CCN or Nickname is linked to details of the investigation, including location and date of incident. |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 21. Report of Investigation (ROI). | C to S | Declassify 10 years from classification date | 1.4(a) | See NOTE 1, 2, and 3. |
| 22. Number and Category of CI/CE cases -- open, closed and pending -- within | C to S | Declassify 10 years from date info is classified | 1.4(a) | Statistics by MSC or Category are CONFIDENTIAL Total INSCOM |

| | | | | |
|---|---|---|---|---|
| USCENTCOM and by Components. | | | | statistics are SECRET. |
| 23. Investigative techniques for a specific case. | C to S | May be exempted : Declassify 10 to 25 years from date info is classified if information reveal actual U.S. military war plans that remain in effect; including foreign government information that would seriously and demonstrably undermine ongoing diplomatic activities of the United States | 1.4(a)<br>1.4(c)<br>1.4(d) | See NOTE 1. The following items will also be classified SECRET: overall investigative plan, Procedure requests, CIOCs or CISOCs, and technical CI support. |
| 24. Fact that the USCENTCOM and subordinate units engage in offensive CI operations (OFCO). | S//NOFORN | Declassify 10 years from date info is classified | 1.4(a) | See NOTE 4 |
| 25. Source or operation/program nickname. | U or S//NOFORN | Declassify 10 years from date info is classified | 1.4(a)<br>1.4(c) | UNCLASSIFIED when standing alone. SECRET /NOFORN when associated with Identifying information. See NOTE 4 |
| 26. Memorandums of Agreements or Understanding between CI/HUMINT units and assets. | S//NOFORN | Declassify 10 years from date info is classified | 1.4(c) | See NOTE 4. |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 27. Information related to those activities of CI assets covered under the provisions of DoDI 5240.9. | S//NOFORN | May be exempted : Declassify 10 to 25 years from date info is classified if the identity of a confidential source, or a human intelligence source, or information about the application of an intelligence source | 1.4(a)<br>1.4(c) | See NOTE 4. |

| | | | | |
|---|---|---|---|---|
| | | or method | | |
| 28. Consolidated reports on activities covered under the provisions of DoDI 5240.9 | S//NOFORN | May be exempted : Declassify 10 to 25 years from date info is classified if the identity of a confidential source, or a human intelligence source, or information about the application of an intelligence source or method | 1.4(a)<br>1.4(c)<br>1.4(d) | See NOTE 4. |
| 29. Summaries of individual cases. | S//NOFORN | Declassify 10 years from date info is classified | 1.4(a) | See NOTE 4. |
| 30. Aggregate statistics disclosing no operational details. | C<br>to<br>S//NOFORN | Declassify 10 years from date info is classified | 1.4(a) | CONFIDENTIAL /NOFORN when showing number of active/inactive OFCO cases standing alone or by region/CINC AO (i.e.,EUCOM, Europe, CENTCOM, Asia, etc.). SECRET/NOFORN when showing numbers of operations against a specific country and at all other times. See NOTE 4. |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 31. Consolidated listings of CI/HUMINT assets or operations. | S//NOFORN | May be exempted : Declassify 10 to 25 years from date info is classified if information reveal actual U.S. military war plans that remain in effect; including foreign Gov't information that would seriously and demonstrably | 1.4(a)<br>1.4(b)<br>1.4(c)<br>1.4(d)<br>1.4(g) | See NOTE 4. |

| | | | | |
|---|---|---|---|---|
| | | undermine ongoing diplomatic activities of the United States | | |
| 32. CDR USCENTCOM or Component CDR PIRs | C<br>To<br>S//NOFORN | Declassify 10 years from date info is classified | 1.4(a) | CONFIDENTIAL when disassociated from operation or source. SECRET/NOFORN at all other times. See NOTE 4. |
| 33. Modus Operandi (MO) of U.S. Intelligence Agencies. | C<br>To<br>S//NOFORN | May be exempted : Declassify 10 to 25 years from date info is classified if information reveals actual U.S. military war plans that remain in effect | 1.4(a)<br>1.4(c)<br>1.4(d)<br>1.4(g) | See NOTE 4. |
| 34. MO of Foreign Intelligence Entities(FIE) in specific cases. | C<br>To<br>S//NOFORN | Declassify 10 years from date info is classified | 1.4(a)<br>1.4(b) | See NOTE 4. |
| 35. Vetting or Asset validation Procedures. | C | Declassify 10 years from date info is classified | 1.4(a) | See NOTE 4. |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 36. Biographical background and personality data. | S//NOFORN | May be exempted : Declassify 10 to 25 years from date info is classified if the identity of a confidential source, or a human intelligence source, or information about the application of an intelligence source or method | 1.4(a)<br>1.4(c)<br>1.4(d) | See NOTE 4. |
| 37. CI support to Force Protection: If minor vulnerabilities | C | 5 years or when the vulnerability is corrected. | 1.4(a) | |

| | | | | |
|---|---|---|---|---|
| are identified. | | | | |
| 38. CI support to Force Protection: If major vulnerabilities are identified | S | Up to 25 years if information revealed would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to national security | 1.4(a) | May be classified higher, depending on the assessed unit's SCG. In some rare circumstances, vulnerabilities and/or countermeasures -- even after they have been corrected -- could still compromise the activity, program or operation being assessed if they became known to FIS/HOIS. |
| 39. CI support to Special Access Programs (SAPs) and Special Mission Units (SMUs). | U to S | Declassify 10 to 25 years from date info is classified if information would impair the application of state-of-the-art technology with a U.S. weapons system | 1.4(a) | Identities of supported programs, activities or units may be classified, depending on their sensitivity. Consult the supported program's SCG. |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 40. CI support to Acquisition System Protection Program (ASPP). | U | | 1.4(a) | Fact that CI supports ASPP is UNCLASSIFIED. |
| 41. Request for CI Technical Services (COMSEC Monitoring/TSCM/TEMPEST/Polygraph/Counter-SIGINT support. | U to S | Declassify 10 years from date info is classified | 1.4(a) | UNCLASSIFIED unless the dates of the service or the phone lines to be monitored are listed; SECRET prior to and during the service; May be classified higher, depending on the monitored |

| | | | | |
|---|---|---|---|---|
| | | | | unit's SCG. |
| 42. CI Technical Services Reports | U to C | Declassify 5 years from date info is classified | 1.4(a) | UNCLASSIFIED if no vulnerability or security violations are identified; CONFIDENTIAL if vulnerabilities or security violations are identified. May be classified higher, depending on the monitored unit's SCG. |
| 43. Information concerning CI/HUMINT and other sensitive intelligence sources and methods | S<br>to<br>S//NOFORN | Declassify 25 years from Date info is classified | 1.4(a) | SECRET if no source information or methods are identified or discussed |
| 44. Intelligence information obtained from CI/HUMINT activities | C<br>to<br>S//NOFORN | Declassify 25 years from Date info is classified | 1.4(a) | Sensitive source operations and information may be classified higher or carry restricted access if requested |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 45. Information on the coding and registration of sources (i.e., Basic Source Data or BSD) with the Defense Source Registry (DSR), the Source Operations Management Module (SOMMS, or any other theater source registry) | S//NOFORN | Declassify 25 years from Date info is classified | 1.4(a) | Sensitive source operations and information may be classified higher or carry restricted access if requested |

NOTES:
1 - (U) All CI/CE operational activity – namely investigations, projects and operations as defined in AR 381-20 -- will be classified a minimum of CONFIDENTIAL unless a higher classification is imposed elsewhere in this SCG or based on material derived from another SCG.

2 - (U) Classify SECRET for Category I and II cases and those Category VI cases where foreign intelligence services are suspected or confirmed.

3 - (U) May be classified higher based on another SCG, a tasking document, or if so specified in an approved CIOC/CISOC.

4 - (S//NF) The NOFORN caveat does not apply to those countries involved in approved bilateral /multilateral Double Agent Operations as specified in the approved CIOC. In lieu of the "NOFORN" caveat as specified in this SCG, the material will be marked "US AND [list the appropriate country] ONLY".

NOTE: See DoD C-5240.8, Department of Defense Counterintelligence Security Classification Guide for additional classification areas. Information classified by DoD C-5240.8 should be marked as follows:

DERIVED FROM: DoD C-5240.8
DECLASSIFY ON: Insert Date Directed by Guide

APPENDIX F

| OPERATIONS (CCJ3-C) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Documents identifying Near Real Time (NRT) track data. Documents identifying Position, Location and Identification of US and coalition forces | Confidential | 10 years | 1.4 (a,g) | May be classified higher if it incorporates information of a higher classification or upon direction of an OCA. |
| 2. Near real time friendly force position, location and identification (PLI) | Mission Dependent (Per JROCM, can start out as unclassified and may be classified higher by OCA depending on the mission.) | 10 yrs or at the conclusion of the operation (i.e. OPLAN COMPLETED). | 1.4 (a,g) | Combat operations is an environment in which the unauthorized disclosure of friendly forces near-real time (NRT) position, location and identification data would place our forces and national security at risk. |
| 3. Friendly Force Position, Location and Identification (PLI) Data during Humanitarian Assistance Operations. | U(FOUO) | Upon movement completion or termination of operation. | 1.4 (a,g) | In a non-hostile environment, the position, location and identification (PLI) of friendly force data will normally be Unclassified. However, the data must be protected in accordance with FIPS-140-2 and may be classified up to secret by OCA, i.e. In some circumstances where the aircraft are taking off from may be classified. |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G

| OPERATIONS (CCJ3-IO) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Exploitable critical or sensitive unclassified information in OCONUS areas or online | C | Upon correction, elimination of weakness, or 10 years, whichever is sooner | 1.4(g) | |
| 2. General OPSEC countermeasures | U | N/A | N/A | |
| 3. Loss of critical sensitive unclassified material | C | Upon identification and mitigation or following completion of damage assessment, whichever is later | 1.4(g) | |
| 4. Weaknesses in the application of OPSEC measures for safeguarding sensitive information on USCENTCOM official websites | C | Upon mitigation of weakness or completion of the operation, whichever is sooner | 1.4(g) | |
| 5. Internet-based Military Information Support Operations (MISO) | C | Declassify 10 years from date info is classified | 1.4(a) | |
| 6. Regional Web Interaction Program (RWIP) | S//REL GBR | N/A | 1.4(a) | |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H

| OPERATIONS (CCJ3-IAG) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Names of Reward Recipients/Informants | U or up to S | Declassify 25 years from the date info is classified | | UNCLASSIFIED/FOUO if SCI#, or OTS# used. SECRET if *Full Name of Recipient used. The Rewards Program is not an Intelligence Program and is not intended to replace any Intelligence Program. |
| 2. Consolidated Rewards List | U | N/A | | Names of HVIs, the cache items discovered, and rewards amounts are UNCLASSIFED/FOUO |
| 3. Reward Nomination Message | S//REL TO USA, ISAF, NATO<br>U | Declassify 25 years from the date info is classified | | UNCLASSIFIED/FOUO if possible for widest dissemination. Only intelligence up to REL TO should be used at maximum |
| 4. HVI Reward Nomination Packages (which includes intelligence) | S//REL TO USA, ISAF, NATO<br>U | Declassify 25 years from the date info is classified | | Only intelligence up to REL TO should be used at maximum |
| 5. FRAGOs / Genadmin Messages | S//REL TO USA, ISAF, NATO<br>U | Declassify 25 years from the date info is classified | | UNCLASSIFIED/FOUO if possible for widest dissemination<br>Only intelligence up to REL TO should be used at maximum |
| 6. Taskers: ESPs / memos / information papers / talking points / case studies / RFIs | S//REL TO USA, ISAF, NATO<br>U | Declassify 25 years from date info is classified or can be marked upon execution of operation | | UNCLASSIFIED/FOUO if possible for widest dissemination<br>Only intelligence up to REL TO should be used at maximum |
| 7. Reward Authorization List (RAO) | U | N/A | | Monthly list provided by CENTCOM to the AOR |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |

| | | | | |
|---|---|---|---|---|
| 8. Pay Vouchers | U | N/A | | All Financial Documents (EX: DD 1081) are UNCLASSIFIED/FOUO unless packet contains higher classification from other documents |
| 9. Quarterly/End of Year Reports | U up to S//NOFORN | Declassify 25 years from the date info is classified | | Classification depends on the classification level of intelligence information in document |

WARNING: Rewards documents that contain derivative classified information and controls must contain at least the same level of classification and controls as the information from which it was derived

APPENDIX I

| OPERATIONS (CCJ3-O) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | COMMENTS |
| 1. Commander's Update Brief (CUB) and Component Commanders Brief (CCB) | S CUB - S//REL TO USA, FVEY to GCTF depending on slide package loaded for brief.<br>CCB – S//REL TO USA, ACGU | Declassify 10 years from date info is classified | 1.4 (a) | Displayed brief is S or higher, adjusted to Rel for posting in shared folders |
| 2. Current Ops briefings / CDR and J3 Trip books | S<br>S//REL TO USA, ACGU or U | Declassify 10 years from date info is classified | 1.4 (a)<br>1.4 (b)<br>1.4 (d) | Classification depends on audience |
| 3. FRAGOs / Genadmin messages | S<br>S//REL TO USA, ACGU<br>S//REL TO USA, GCTF<br>S//REL TO USA, FVEY | Declassify 10 years from date info is classified | 1.4 (a) | Classification depends on target audience. Code words/mission nicknames are UNCLASSIFIED when not associated with mission details |
| 4. Taskers: ESPs / memos / information papers / talking points / RFIs | S<br>S//REL TO USA, ACGU<br>S//REL TO USA, GCTF<br>S//REL TO USA, FVEYU | Declassify 10 years from date info is classified | 1.4 (a) | Classification depends on target audience. Code words/mission nicknames are UNCLASSIFIED when not associated with mission details |
| 5. Weather briefing slides | S//REL TO USA GCTF | Declassify 10 years from date info is classified or 7 days after the event, Mark for Manual Release (MR) | 1.4 (a) | Weather forecasts are not classified. Wx Impacts to operations and wx associated with classified locations are classified, as appropriate |
| 6. SIGACT Event Summaries | S//REL (as appropriate) or U | Declassify 10 years from date info is classified or 7 days after the event (MR) | 1.4 (a) | UNCLASSIFIED after the info has been sanitized of specific unit, friendly casualties, battle damage, and other sensitive operational information |

| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | COMMENTS |
|---|---|---|---|---|
| | | | | |
| 7. SIGACTs related to fact of and general type (vehicle-borne, etc) of IED attack at specific location on specific date | S or S//REL (as appropriate) | Mark for Manual Release (MR) and declassification 24 hrs after the event | 1.4 (a) | UNCLASSIFIED after the info has been sanitized of specific unit, friendly casualties, battle damage, and other sensitive information. DO NOT reveal details of IED attacks such as insurgent tactics and their effectiveness |
| 8. SIGACTs related to the fact of discovery of IED | S or S//REL (as appropriate) | Mark for Manual Release (MR) and declassification 24 hrs after the event | 1.4 (a) | Details on how IED was discovered CANNOT be automatically declassified. DO NOT reveal, details of Coalition Forces IED countermeasures |
| 9. SIGACTs related to fact of and type of terrorist/insurgent attack at specific location on specific date | S or S//REL (as appropriate) | Mark for Manual Release (MR) and declassification 24 hrs after the event | 1.4 (a) | UNCLASSIFIED after the info has been sanitized of specific unit, friendly casualties, battle damage, and other sensitive information. |
| 10. Products derived from SIGACTs which show aggregate, rough statistics on IEDs (total number found type, total detonated | S or S//REL (as appropriate) | Mark for Manual Release (MR) and declassification 24 hrs after the event | 1.4 (a) | Details of casualties linked to specific IEDs or attacks, to include location or timeframe CANNOT be automatically declassified. |
| 11. Operational code word(s) when identified with mission operations | S or S//REL (as appropriate) | Declassify upon completion of movement or termination of operations (MR) | 1.4 (a) | Code words/mission nicknames are UNCLASSIFIED when not associated with mission details |
| 12. Concept of operations (CONOPS), Operations Orders (OPORD) or Fragmentary Orders (FRAGOs) | S or S//REL (as appropriate) | Declassify 10 years from date info is classified or can be marked upon execution of operation (MR) | 1.4 (a) | An FDO may disclose or release information to the HN when required to perform a mission. The timing should maximize training & planning, but minimize operational risk. |
| INFORMATION | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |

| REVEALING | | | | |
|---|---|---|---|---|
| 13. Specific components or MSCs' goals, aims or intentions | S or S//REL (as appropriate) | Declassify 10 years from date info is classified or can be marked upon execution of operation (MR) | 1.4 (a) | |
| 14. Movement of ammunition, aircraft, personnel, units, or comm equipment | S or S//REL (as appropriate) | Declassify upon completion of movement or termination of operations (MR) | 1.4 (a) | An FDO may disclose or release to the HN when required to perform a mission. The timing should maximize training & planning, but minimize operational risk. J3-O may downgrade to meet operational requirements or provide access to this information to necessary support personnel after assessing operation risk. |
| 15. Date and time mission/operation begins | S or S//REL (as appropriate) | Declassify upon completion of movement or termination of operations (MR) | 1.4 (a) | An FDO may disclose or release to the HN when required to perform a mission. The timing should maximize training & planning, but minimize operational risk. |
| 16. Time lines/ schedules | S or S//REL (as appropriate) | Declassify 10 years from date info is classified or upon execution of operation (MR) | 1.4 (a) | FDO may disclose or release timelines to HN when required to perform a mission. The timing should maximize training & planning, but minimize operational risk. J3-O may downgrade to meet operational requirements or provide access to information necessary to support personnel after assessing operational risk. |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 17. Specific | S or S//REL (as | Declassify 10 years | 1.4 (a) | FDO may disclose or |

| | | | | |
|---|---|---|---|---|
| locations, grids, or geo-coords to be used | appropriate) | from date info is classified or upon execution of operation (MR) | | release timelines to HN when required to perform a mission. The timing should maximize training & planning, but minimize operational risk. J3-O may downgrade to meet operational requirements or provide access to information necessary to support personnel after assessing operational risk. |
| 18. Implementing conditions and decision points | S or S//REL (as appropriate) | Declassify 10 years from date info is classified or can be marked upon execution of operation (MR) | 1.4 (a) | FDO may release to HN when required to perform a mission. The timing should maximize training & planning, but minimize operational risk. |
| 19. Operation specific rules of engagement (ROE) | S or S//REL (as appropriate) | Declassify 10 years from date info is classified or upon execution of operation (MR) | 1.4 (a) | General theater ROE statements and ROE cards are unclassified. ROE may have to be sanitized before release. |
| 20. Operational capabilities/shortfalls | S or S//REL (as appropriate) | Declassify 10 years from date info is classified | 1.4 (g) | |
| 21. Operation readiness (alert) time (i.e. emplacement, loading, firing, QRF dispatch times, etc.) | S or S//REL (as appropriate) | Declassify 10 years from date info is classified or upon execution of operation (MR) | 1.4 (a) | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 22. Specific operational information | U or S or S//REL (as appropriate) | Declassify 10 years from date info is classified; or upon execution of operation | 1.4 (a) | UNCLASSIFIED if the info: 1) describes a past event and is expressed in generic terms, 2) |

| | | | | |
|---|---|---|---|---|
| | | (MR) see comment | | provides no indicators of potential future ops, 3) does not provide specific locations, unit data, TTPs, capabilities, or source info 4) does not embarrass any Coalition members, 5) does not violate any of the above if released over time or in compilation |
| 23. Overall force structure with total personnel strength figures and percentage of personnel fills | U or C//REL (as appropriate) | Declassify 10 years from date info is classified | 1.4 (a) | Strength of all deployed forces is CONFIDENTIAL; Individual unit strength is UNCLASSIFIED |
| 24. Techniques, limitations, and effectiveness of psychological ops | S or S//REL (as appropriate) | Declassify 10 years from date info is classified | 1.4 (a) | Releasable only to participants with a strict "Need to Know" |
| 25. Supporting Intel and counter Intel plans/operations | S or S//REL (as appropriate) | Declassify 10 years from date info is classified | 1.4 (a)<br>1.4 (g) | Releasable only to participants with a strict "Need to Know" |
| 26. Fratricide issues | U or S or S//REL (as appropriate) | Public release authority rests with component commanders | 1.4 (a) | |
| 27. Accident and safety data | U | Should only be distributed to Components and non-Coalition countries only with a strict "Need to Know | 1.4 (a) | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 28. Targeting methodology and target selection process | S or S//REL (as appropriate) | Declassify 10 years from date info is classified | 1.4 (a) | Releasable only to participants with a strict "Need to Know" |
| 29. Command | U | UNCLASSIFIED | 1.4 (a) | |

| | | | | |
|---|---|---|---|---|
| relationships, agreements and MOU. | | unless classified IAW "Specific details of Coalition plans" above | 1.4 (g) | |
| 30. Effects Synchronization Committee (ESC) Briefing Slides, Effects Synchronization Working Group agenda & Post meeting notes | S<br>S//REL TO USA, ACGU<br>S//REL TO USA, GCTF<br><br>S//NOFORN | Declassify 10 years from date info is classified | 1.4 (d) | Classification depends on target audience. |
| 31. Near real time friendly force position, location and identification (PLI) TRACK DATA DURING COMBAT OPERATION. | S | 10 yrs or at the conclusion of the operation (i.e. OPLAN COMPLETED). Combat operations is an environment in which the unauthorized disclosure of friendly forces near-real time (NRT) position, location and identification data would place our forces and national security at risk. | 1.4 (g) | In a hostile environment the systems must be capable of protecting Blue Force Tracking Data (to include Coalition Partners) to a level merited by classification. USCENTCOM is the OCA for Friendly Force Position, Location, and Identification (PLI) data within its AOR. However, Commander may downgrade to meet operational requirement or to provide access to this information to personnel. On need-to-now information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 32. Friendly Force Position, Location and Identification (PLI) Data during Humanitarian Assistance Operations. | U(FOUO) | Upon movement completion or termination of operation. | 1.4 (g) | In a non-hostile environment, the position, location and identification (PLI) of friendly force data will normally be Unclassified. However, |

| | | | | |
|---|---|---|---|---|
| | | | | the data must be protected in accordance with FIPS-140-2. |
| 33. Consequence Management of Friendly Force Position, Location and Identification (PLI) Data. | U or up to S | 10 yrs if data/Information deemed classified. The unauthorized disclosure of U.S. participation in certain consequences management operation may cause damage to U.S. National Security by revealing sources, methods and capabilities | 1.4 (g) | U.S. Forces participation in consequences management Operations will normally be unclassified. However, the nature of the event or U.S. Forces participation may require participation and position, location an identification data to be classified |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX J

| STRATEGIC DEPLOYMENT (CCJ3-S) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. C-Date/calendar date association | S | 3 years after completion | 1.4(a) | |
| 2. Concept of operations | S | 1 year after completion | 1.4(a) | Confidential upon execution |
| 3. Exercise name | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 4. Exercise/operation location | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 5. 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 |
| 6. exercise/operation name associated with participating units | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 7. Operation code words | S | 1 year after completion | 1.4(a) | Confidential upon execution |
| 8. Participation of a specific individual in operation or exercise | U | N/A | N/A | |
| 9. Participating units, including type, 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 |
| 10. Units/HN association | S | 1 year after completion | 1.4(a) 1.4(d) | Confidential upon execution |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX K

| LOGISTICS AND ENGINEERING (CCJ4) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Analysis and impact of all USCENTCOM AORs | S/REL/FVEY | Upon completion of mission | 1.4(d) / 1.4(g) | Negotiations of construction projects, AIK, customs issues, etc |
| 2. 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) | |
| 3. Characteristics of U.S. weapons and related sustainability | S | 10 years | 1.4(a) | May be classified higher upon direction of an OCA |
| 4. Deployment/redeployment of units | S | 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 |
| 5. Force protection threat analysis | S | Upon completion of mission | 1.4(g) | Includes intelligence efforts and threat weapons |
| 6. 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 |
| 7. MOBSTR-B | S | Upon completion of mission | 1.4(g) | Location/ capabilities of relay system for U2 |
| 8. Movement of ammunition, aircraft, personnel, units, or communications equipment | S | Upon completion of mission | 1.4(a) / 1.4(g) | May be classified higher upon direction of an OCA |
| 9. Movement of sensitive or critical supplies/personnel | S | Upon completion of mission | 1.4(a) / 1.4(g) | May be classified higher upon direction of the CCJ4/7 OCA |
| 10. 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) |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |

| | | | | |
|---|---|---|---|---|
| 11. Proposed U.S. positions or strategy of negotiations | S/REL/FVEY | Upon completion of mission | 1.4(a) / 1.4(d) | Negotiations of construction projects, assistance in kind (AIK), customs issues, etc. |
| 12. War reserve stockage data | S/REL/FVEY | 10 years | 1.4(a) / 1.4(g) | |

APPENDIX L

| STRATEGY, PLANS, AND POLICY (CCJ5) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Beddown sites | S | 10 years or upon plan execution, if executed | 1.4(a) | |
| 2. Capabilities-based munitions requirements | S | 10 years | 1.4(a) | |
| 3. Chemical/biological weapons and proliferation plans | S | 10 years | 1.4(a) / 1.4(h) | |
| 4. Command and control relationships | U | N/A | N/A | |
| 5. Commander's intent | S | 10 years | 1.4(a) | Confidential upon plan execution |
| 6. Deception plans for operations | TS | 10 years | 1.4(a) | |
| 7. Defended assets list (DAL) | S | 10 years | 1.4(a) | |
| 8. Essential elements of friendly information (EEFI) | S | 10 years | 1.4(a) | Complete detailed list |
| 9. Force lists | S | 10 years | 1.4(a) | Confidential |
| 10. HN participation | S | 10 years or upon plan execution, if executed | 1.4(a) / 1.4(b) | |
| 11. Joint monthly readiness review (JMRR) | S | 10 years | 1.4(a) | |
| 13. Location and designation of USCENTCOM representatives | U | N/A | N/A | |
| 14. Mission statements | S | 10 years | 1.4(a) | Confidential upon plan execution |
| 15. NBC operations | S | 10 years | 1.4(a) 1.4(h) | |
| 16. Plan briefs | S | 10 years | 1.4(a) | |
| 17. Plan phasing | S | 10 years | 1.4(a) | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |

| | | | | |
|---|---|---|---|---|
| 18. Planning directives | S | 10 years | 1.4(a) | Confidential upon plan execution |
| 19. Planning milestones, internal suspense dates | U | N/A | N/A | |
| 20. Rules of engagement | S | 10 years or upon plan execution, if executed | 1.4(a) | |
| 21. Strategic concepts | S | 10 years | 1.4(a) | |
| 22. TPFDD plan identifiers, except: | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 23. Aggregate tonnage/pax | U | N/A | N/A | |
| 24. U.S. unit name and destination combined | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 25. U.S. unit name with EAD/LAD | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 26. U.S. unit name with UIC/ULN | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 27. ULN and destination | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 28. ULN and EAD/LAD | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 29. Origin, UIC, and ULN | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 30. Flight plans for logistics support | S | Upon execution | 1.4(a) | If classification/ declassification |

| | | | | |
|---|---|---|---|---|
| | | | | instructions are not specified by JCS/HN |
| 31. War Plan Short title (Number) displayed with Long Title , nickname, name of country or displayed with an image or graphic of the country related to the plan | S | Declassify 10 years from date info is classified<br><br>May be manually reviewed after plan execution | 1.4 (a) | Any linkage of a War Plan Number to the country it addresses is classified Secret Sensitive planning efforts may be classified higher by direction of the OCA |
| 32. War plan short title or long title standing alone | U | N/A | N/A | |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX M

| DELIBERATE WAR PLANS (CCJ5-P) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Characteristics of U.S. weapons and related sustainability | S | 10 years | 1.4(a) | May be classified higher upon direction of an OCA |
| 2. Communications effectiveness, sustainability, limitations | S | 10 years | 1.4(a) | |
| 3. Concept of operations including order of battle, execution circumstances, operating locations, resources required, tactical maneuvers, deployments, action and objectives | S | 10 years | 1.4(a) | Confidential upon plan execution |
| 4. DEFCON meaning and status | S | 10 years | 1.4(a) | |
| 5. Synchronization matrices | S | 10 years | 1.4(a) | |
| 6. Plan(s) timelines | S | 10 years | 1.4(a) | |
| 7. Flexible deterrent options | S | 10 years | 1.4(a) | |
| 8. Estimates of operational effectiveness of intelligence, counterintelligence, rescue, and reconnaissance | S | 10 years | 1.4(a) | |
| 9. Limitations and vulnerabilities of U.S. forces in the combat area | S | 10 years | 1.4(g) | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |

| | | | | |
|---|---|---|---|---|
| 10. 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 |
| 11. Nuclear weapons; potential use of | S | 10 years | 1.4(a)<br>1.4(h) | |
| 12. Operation code words | S | 10 years | 1.4(a) | |
| 13. 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 |
| 14. Plan classification guide | C | 10 years or upon plan execution, if executed | 1.4(a) | |
| 15. Planning assumptions | S | 10 years or upon plan execution, if executed | 1.4(a) | |
| 16. 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)<br>1.4(d) | |
| 17. Friendly centers of gravity | S | 10 years | 1.4(a) | |
| 18. War termination objectives | S | 10 years | 1.4(a) | |
| 19. End state of plan | S | 10 years | 1.4(a) | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 20. Target area weather information | S | 10 years or upon plan execution, if executed | 1.4(a) | |

| | | | | |
|---|---|---|---|---|
| 21. Top secret options; discussion of | TS | 10 years | 1.4(a) | |
| 22. Limitations and vulnerabilities of U.S. | S | 10 years | 1.4(g) | |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX N

| COMMAND AND CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS (CCJ6) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Communications networks, users, frequencies, call signs, HJ times, and identification of net control stations | C//REL (as appropriate) | Declassify 10 years from date info is classified | 1.4(a)<br>1.4(g) | May require higher classification depending upon the system. Disclosure will facilitate enemy disruption of C2 capabilities |
| 2. COMSEC incidents/violations | C | Declassify 10 years from date info is classified or can be marked upon execution of operation | 1.4(g) | Per E.O. 13526, releasable only after Manual Review. Disclosure would ease the exploitation of the individual networks |
| 3. Composite list of COMSEC short titles | C | Declassify 10 years from date info is classified or can be marked upon execution of operation | 1.4(c) | Per E.O. 13526, releasable only after Manual Review. Disclosure would ease the exploitation of the individual networks |
| 4. Cryptology | S | 10 years | 1.4(c) | |
| 5. Communication outages that degrade command and control capability | S//REL TO USA, GCTF | Declassify 10 years from date info is classified or can be marked upon execution of operation | 1.4(g) | Releaseability dependant on theater; Per E.O. 13526, releasable to ISAF / NATO on manual review. Disclosure could provide assessment of hostile actions that may have caused the outage. |
| 6. Computer (SIPR, GCCS, CENTRIXS, NIPR) User ID | U//FOUO | N/A | N/A | |
| INFORMATION | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |

| REVEALING | | | | |
|---|---|---|---|---|
| 7. Scheduled down times of communications systems | S//REL TO USA, GCTF | Declassify 10 years from date info is classified or can be marked upon execution of operation | 1.4(g) | Releaseability dependent on theater; Per E.O. 13526, releasable to ISAF / NATO on manual review. Disclosure could provide assessment of an individual node's importance in the network. |
| 8. Computer (SIPR, GCCS, CENTRIXS, NIPR) Password | S/<br>or<br>S//REL TO USA, GCTF | Declassify 10 years from date info is classified or can be marked upon execution of operation | 1.4(a) | Releasable to individual user only; Dependent on classification of computer system. Disclosure will allow unauthorized access to computer system. |
| 9. Specific locations of deployed communications units | C//REL<br>TO USA, GCTF | Upon redeployment | 1.4(a)<br>1.4(g) | Releaseability dependent on theater; Per E.O. 13526, releasable to ISAF / NATO on manual review. Disclosure could provide assessment of an individual node's importance in the network |
| 10. Specific location or countries planned for employment of elements of SWA extensions to the Defense Information Communications Agency Global Information Grid or Theater Information Grid | C//REL TO USA, GCTF | Upon redeployment | 1.4(a)<br>1.4(g) | Releaseability dependent on theater; Per E.O. 13526, releasable to ISAF / NATO on manual review. Disclosure could provide assessment of an individual node's importance in the network |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 11. Specific locations or | S | 10 years | 1.4(d) | |

| | | | | |
|---|---|---|---|---|
| countries in which USCENTCOM Joint C4 Theater Information Grid (TIG)are employed | | | | |
| 12. Specific locations of deployed communications units | S//REL TO USA, GCTF | Upon redeployment | 1.4(a)<br>1.4(g) | Ability to release depends on theater; Per E.O. 13526, releasable to ISAF / NATO on manual review. Disclosure could provide assessment of an individual node's importance in the network |
| 13. Details revealing force locations, by type, for war plan employment of CENTCOM controlled communications assets | S//REL TO USA, GCTF | Upon redeployment | 1.4(c)<br>1.4(g) | Ability to release depends on theater; Per E.O. 13526, releasable to ISAF/ NATO on manual review. Disclosure could provide assessment of an individual node's importance in the network |
| 14. Specific locations or countries in the AOR in which communication equipment is identified as supporting the USCENTCOM Joint C4 Theater Information Grid | S | 10 years | 1.4(d) | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 15. Identification of an operational shortfall or limitation In war- | S | Upon correction | 1.4(g) | |

| | | | | |
|---|---|---|---|---|
| fighting capabilities of USCENTCOM Joint C4 Theater Information Grid (TIG). | | | | |
| 16. Details of the capability required to achieve the initial operational capability of USCENTCOM Joint C4 TIG. | S | Upon full operational capability | 1.4(g) | |
| 17. A description of the USCENTCOM Joint C4 Theater Information Grid (TIG)system and details of the capability required to achieve full operational capability | U//FOUO | N/A | N/A | Description includes diagrams or drawings depicting the details of deployed systems. |
| 18. A description of the composition of a USCENTCOM Joint C4 Theater Information Grid (TIG)node at full operational capability | U//FOUO | N/A | N/A | Description includes diagrams or drawings depicting the details of deployed systems. |
| 19. Characteristics of the USCENTCOM Joint C4 Theater Information Grid (TIG). | U | N/A | N/A | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 20. Cost/Budget data on the USCENTCOM Joint C4 Theater Information Grid (TIG). | U | N/A | N/A | |

| | | | | |
|---|---|---|---|---|
| 21. Identification of the agencies responsible for the various aspects of system acquisition, implementation, operation, and maintenance | U | N/A | N/A | |
| 22. Required capability dates, initial operational capability, and full operational capability dates | S | Upon execution | 1.4(a) | If classification/ declassification instructions are not specified by JCS/HN |
| 23. Frequencies lists | U | N/A | N/A | |
| 24. Contingency and Operational Joint Communications Electronics Operating Instructions (JCEOI) | S | When superseded | 1.4(a) | Unclassified for training within the U.S. Releasable to MNF when part of Coalition |
| 25. 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) | Releasable to MNF when part of the Coalition. List of frequencies alone are Unclassified |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 26. 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 | U | N/A | N/A | Information required to be released is considered FOUO (DOD 5400.7-R) |

| | | | | |
|---|---|---|---|---|
| the frequency (Example: Land Mobile Radio Communications) | | | | |
| 27. Joint Restricted Frequency Listings (JRFL) | S | When superseded | 1.4(a) / 1.4(c) | Releasable to MNF when part of the Coalition. Determined by Command Electronic Warfare Officer (EWO) |

APPENDIX O

| EXERCISE & TRAINING (CCJ7) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| Exercises (CCJ7) | → | → | → | Separate classification guidance shall be issued by CCJ7 for exercises. CCJ7 will issue a by-country yearly guide or a guide for each specific exercise. For further information, contact CCJ7 |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX P

| ANALYSIS & REQUIREMENTS (CCJ8-AR) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Supporting data and products of analysis of the Joint Planning and Execution System relating to USCENTCOM plans or operations | S | 10 years | 1.4(a) | May be classified higher or lower if it incorporates information of a higher or lower classification or upon direction of an OCA |
| 2. Supporting data and products of analysis of scientific, technological, or economic matters relating to USCENTCOM plans or operations | S | 10 years | 1.4(e) | May be classified higher or lower if it incorporates information of a higher or lower classification or upon direction of an OCA |
| 3. Supporting data and products of analysis identifying vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to USCENTCOM plans or operations | S | 10 years | 1.4(g) | May be classified higher or lower if it incorporates information of a higher or lower classification or upon direction of an OCA |
| 4. Requirements documents identifying USCENTCOM future operational needs | S | 10 years | 1.4(a)<br>1.4(b)<br>1.4(e)<br>1.4(g) | |
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |

| | | | | |
|---|---|---|---|---|
| 5. Documents identifying Urgent Operational Needs (UON) or Joint Urgent Operational Needs (JUON) | S | 10 years | 1.4(a)<br>1.4(c)<br>1.4(e)<br>1.4(g) | May be classified higher or lower if it incorporates information of a higher or lower classification or upon direction of an OCA |
| 6. Data files, plans files, and products of modeling and simulation in support of USCENTCOM War Plan development | S | 10 years | 1.4(a)<br>1.4(b)<br>1.4(c)<br>1.4(g) | May be classified higher or lower if it incorporates information of a higher or lower classification or upon direction of an OCA |
| 7. Supporting data and assessments of the Theater Campaign Plan, Campaign Plans, Major Operations | S | 10 years | 1.4(a)/<br>1.4(b)/<br>1.4(g) | May be classified higher or lower if it incorporates information of a higher or lower classification or upon direction of an OCA |
| 8. Supporting data and products relating to the munitions requirements process in support of the USCENTCOM Theater Strategy. | S | 10 years | 1.4(a)/ | May be classified higher or lower if it incorporates information of a higher or lower classification or upon direction of an OCA |

APPENDIX Q

| SCIENTIFIC ADVISOR (CCJ8-ST) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Vulnerabilities of new military technologies | S | 10 years or upon correction, if corrected | 1.4(e)<br>1.4(g) | |
| 2. New operational concepts based on application of new technologies | S | 25 years | 1.4(e) | |
| 3. Requirements documents identifying critical military deficiencies | S | 10 years | 1.4(g) | |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX R

| COMMAND GROUP (CCCC) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Detailed travel itinerary of USCENTCOM Commander | S | Upon completion of travel | 1.4(a)<br>1.4(g) | Classified when information reveals name/title associated with dates/times or locations |
| 2. Detailed travel itineraries of General/Flag officers and civilian equivalent | S | Upon completion of travel | 1.4(a)<br>1.4(g) | Classified when information reveals name/title associated with dates/times or locations |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX S

| CENTCOM DEPUTY COMMANDER – THEATER TRAVEL COORDINATION CELL (CCDC-TTCC) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. 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.) |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX T

| COMMUNICATION INTEGRATION (CCCI) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| Public affairs contingency statement | U | N/A | N/A | |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX U

| PROVOST MARSHAL (JSD) | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. Deployment / redeployment of security augmentation troops when combined with dates and/or locations | U | N/A | 1.4(a)<br>1.4(g) | Classified only during periods of increased threat; Included are numbers of personnel, dates, and locations. |
| 2. Enemy prisoner of war (EPW) information that reveals locations of units or EPW camps; unit strength and/or military capabilities; or number of EPWs | S | Upon completion of operation/ hostilities | 1.4(a)<br>1.4(c)<br>1.4(g) | |
| 3. Physical security vulnerabilities and vulnerability to terrorist attack | S | Upon correction or after 5 years if uncorrected | 1.4(g) | |
| 4. Threat condition | U | N/A | N/A | |
| 5. Detailed terrorist threat level/condition | C | 10 years | 1.4(a)<br>1.4(g) | May be classified higher upon direction of an OCA |
| 6. General terrorist threat information | U | N/A | N/A | All terrorist threat information must contain unclassified tear line for widest dissemination |
| 7. Vulnerability assessments and trends | S | 10 years | 1.4(g) | May be declassified upon resolution of all vulnerabilities without a waiver |
| 8. Purchase request package | U | N/A | N/A | For Official Use Only |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX V

| Electronic Sweeps | | | | |
|---|---|---|---|---|
| INFORMATION REVEALING | CLASSIFICATION | DECLASSIFICATION | REASON | REMARKS |
| 1. General information not revealing any details | C | 10 years | | See AFI 71-19 for strict need-to-know guidance |
| 2. Specific information revealing date range and area to be swept | S | 10 years | | |
| 3. Target area weather information | S | 10 years or upon plan execution, if executed | 1.4(a) | |
| 4. Top secret options; discussion of | TS | 10 years | 1.4(a) | |

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX W

| Equivalent Foreign Security Classifications | | | | |
|---|---|---|---|---|
| Country | TOP SECRET | SECRET | CONFIDENTIAL | OTHER |
| Albania | TEPER SEKRET | SEKRET | IMIREBESUESHE | I KUFIZUAR |
| Argentina | ESTRICTAMENTE SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Australia | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Austria | STRENG GEHEIM | GEHEIM | VERSCHLUSS | |
| Balkans | STROGO POVERLJIVO State SECRET DRZAVA TAJNA | TAJNO Military SECRET VOJNA TAJNA | POVERLJIVO | |
| Belgium(French) | TRES SECRET | SECRET | CONFIDENTIEL | DIFFUSION RESTREINTS |
| (Flemish) | ZEER GEHEIM | GEHEIM | VERTROUWELIJK | BEPERTKE VERSPREIDING |
| Bolivia | SUPERSECRETO or MUY SECRETO | SECRETO CONFIDENCIAL | RESERVADO | |
| Brazil | ULTRA SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Bulgaria | STROGO SEKRENTO | SEKRETEN/ SEKRETNO | POVERITELEN/ OVERITELNO | OGRANICHE (as in Limited) NEPOZVOLEN (Illicit) ZABRANEN (Forbidden) |
| Cambodia | TRES SECRET | SECRET | SECRET/ CONFIDENTIEL | |
| Canada | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Chile | SECRETO | SECRETO | RESERVADO | RESERVADO |
| Columbia | ULTRASECRETO | SECRETO | RESERVADO | CONFIDENCIAL RESTRINGIDO |
| Costa Rica | ALTO SECRETO | SECRETO | CONFIDENCIAL | |
| Croatia | NAJVECI TAJNITAJNI | TAJNI | POVERLJIV | OGRANCIEN |
| Denmark | YDERST HEMMELIGT | HEMMELIGT | FORTROLIGT | TIL TJENESTEBRUG |
| Ecuador | SECRETISIMO | SECRETO | CONFIDENCIAL | RESERVADO |
| El Salvador | ULTRA SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Ethiopia | YEMIAZ BIRTOU MISTIR | MISTIR | KILKIL | |
| Country | TOP SECRET | SECRET | CONFIDENTIAL | OTHER |

| | | | | |
|---|---|---|---|---|
| Finland | ERITTAIN SALAINEN | | | |
| France | TRES SECRET | SECRET DEFENSE | CONFIDENTIEL | DIFFUSION RESTREINTE |
| Germany | STRENG GEHEIM | GEHEIM | VERTRAULICH | |
| Greece | AKP/ AOPPHTON | AOPPHTON | EMITEYTIKON | EPIPIMENH XPHE |
| Guatemala | ALTO SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Haiti | | SECRET | CONFIDENTIAL | |
| Honduras | SUPER SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Hong Kong | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Hungary | SZIGOR'UAN TITKOS | TITKOS | BIZALMAS | |
| Iceland | ALGJORTI | TRUNADARMAL | | |
| India | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Indonesia | SANGAT RAHASIA | RAHASIA | TERBATAS | |
| Iran | BENKOLI SERRI | SERRI | KHEILI MAHRAMANEH | |
| Iraq (English Translation) | ABSOLUTELY SECRET | SECRET | | LIMITED |
| Ireland (Gaelic) | AN-SICREIDEACH | SICREIDEACH | RUNDA | SRIANTA |
| Israel | SODI BEYOTER | SODI | SHAMUR | MUGBAL |
| Italy | SEGRETISSIMO | SEGRETO | RISERVATISSIMO | RISERVATO |
| Japan | KIMITSU | GOKUHI | HI | TORIATSUKAICHUI |
| Jordan | MAKTUM JIDDAN | MAKTUM | SIRRI | MAHDUD |
| Kazakhstan | | | | Use Russian equiv. |
| Korea | KUP PI MIL | KUP PI MIL | KUP PI MIL | |
| Kyrgyzstan | | | | Use Russian equiv. |
| Laos | TRES SECRET | SECRET | SECRET/ CONFIDENTIEL | DIFFUSION RESTREINTE |
| Lebanon | TRES SECRET | SECRET | CONFIDENTIEL | |
| Moldovan (May use Russian Equiv.) | ULTRASECRET | SECRET | CONFIDENTIAL SECRET | RESTRINS |
| Mexico | ALTO SECRETO | SECRETO | CONFIDENCIAL | RESTRINGIDO |
| Country | TOP SECRET | SECRET | CONFIDENTIAL | OTHER |
| Netherlands | ZEER GEHEIM | GEHEIM | CONFIDENTIEEL VERTROUWELIJ | DIENSTGEHEIM |

| | | | | |
|---|---|---|---|---|
| | | | K | |
| New Zealand | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Nicaragua | ALTO SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Norway | STRENGT HEMMELIG | HEMMELIG | KONFIDENSIELL | BEGRENSET |
| Pakistan | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Paraguay | SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Peru | ESTRICTAMENTE SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Philippines | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Poland | TAIJNY SPECJALNEGO | TAJNY | POUFNY | |
| Portugal | MUITO SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Romanian | ULTRASECRET | SECRET | CONFIDENTIAL OR SECRET | RESTRINS |
| Russian | COBEOWEHHO | CEKPETHO | | |
| Saudi Arabia | SAUDI TOP SECRET | SAUDI VERY SECRET | SAUDI SECRET | SAUDI RESTRICTED |
| Spain | MAXIMO SECRETO | SECRETO | CONFIDENCIAL | DIFFUSION LIMITADA |
| Sweden (Red Borders) | HEMLIG | HEMLIG | | |
| Switzerland (Three languages. TOP SECRET has a registration number to distinguish it from SECRET AND CONFIDENTIAL) | | | | |
| Taiwan (No translation in English characters) | | | | |
| Tajikistan (Use Russian equivalent) | | | | |
| Thailand | LUP TISUD | LUP MAAG | LUP | POK PID |
| Turkey | COK GIZLI | GIZLI | OZEL | HIZMET OZEL |
| Turkmenistan (Use Russian equiv.) | | | | |
| Ukraine | TSILKOM SEKRETNE | SEKRETNO | KONFIDENTSIAL'NO | DLYA |
| South Africa | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Afrikaans | UITERS GEHEIM | GEHEIM | VERTROULIK | BEPERK |
| Egypt) | TOP SECRET | VERY SECRET | SECRET | OFFICIAL |
| United Kingdom | TOP SECRET | SECRET | CONFIDENTIAL | RESTRICTED |
| Country | TOP SECRET | SECRET | CONFIDENTIAL | OTHER |
| Uruguay | ULTRA SECRETO | SECRETO | CONFIDENCIAL | RESERVADO |
| Uzbekistan (Use Russian equivalent) | | | | |
| Vietnam | TRES SECRET | SECRET | CONFIDENTIEL | DIFFUSION |

| | | | | |
|---|---|---|---|---|
| | | DEFENSE | DEFENSE | RESTREINTE |
| (Vietnamese) | TOI-MAT | MAT | KIN | TU MAT |

Note: The classifications given above represent the nearest comparable designation that are used to signify degrees of protection and control similar to those prescribed for the equivalent U.S. classification.