

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>



Department of Defense MANUAL

NUMBER 5200.01, Volume 1
February 24, 2012

USD(I)

SUBJECT: DoD Information Security Program: Overview, Classification, and
Declassification

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP). This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526 and E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume:

- (1) Describes the DoD Information Security Program.
- (2) Provides guidance for classification and declassification of DoD information that requires protection in the interest of the national security.
- (3) Cancels Reference (c) and DoD O-5200.1-I (Reference (g)).
- (4) Incorporates and cancels Directive-Type Memorandums 04-010 (Reference (h)) and 11-004 (Reference (i)).

2. APPLICABILITY. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereinafter referred to collectively as the “DoD Components”).

b. Does NOT alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community pursuant to policies issued by the DNI. Consistent with Reference (b), SCI shall be safeguarded in accordance with the policies and procedures issued by the DNI, as implemented by DoD 5105.21-M-1 (Reference (j)) and other applicable guidance.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy, in accordance with Reference (b), to:

a. Identify and protect national security information and CUI in accordance with national level policy issuances.

b. Promote information sharing, facilitate judicious use of resources, and simplify management through implementation of uniform and standardized processes.

c. Classify and declassify national security information as required by References (d) and (f).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosures 3 through 6.


7. INFORMATION COLLECTION REQUIREMENTS

a. The Annual Report on Classified Information referenced in paragraph 7.m. of Enclosure 2 of this Volume has been assigned Report Control Symbol (RCS) DD-INT(AR)1418 in accordance with the procedures in DoD 8910.1-M (Reference (k)).

b. The DoD Security Classification Guide Data Elements, DoD (DD) Form 2024, referenced in section 6 of Enclosure 6 of this Volume has been assigned RCS DD-INT(AR)1418 in accordance with the procedures in Reference (k).

8. RELEASABILITY. UNLIMITED. This Volume is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

9. EFFECTIVE DATE. This Volume is effective upon its publication to the DoD Issuances Website.



Michael G. Vickers
Under Secretary of Defense
for Intelligence

Enclosures

1. References
2. Responsibilities
3. DoD Information Security Program Overview
4. Classifying Information
5. Declassification and Changes in Classification
6. Security Classification Guides

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....8

ENCLOSURE 2: RESPONSIBILITIES.....11

 UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)).....11

 UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)).....11

 DoD CHIEF INFORMATION OFFICER (CIO).....12

 ADMINISTRATOR, DEFENSE TECHNICAL INFORMATION CENTER (DTIC).....12

 DIRECTOR, WHS.....12

 HEADS OF THE DoD COMPONENTS12

 SENIOR AGENCY OFFICIALS13

 HEADS OF DoD ACTIVITIES16

 ACTIVITY SECURITY MANAGER.....17

 TSCO19

 SENIOR INTELLIGENCE OFFICIAL19

 INFORMATION SYSTEMS SECURITY OFFICIALS.....20

ENCLOSURE 3: DoD INFORMATION SECURITY PROGRAM OVERVIEW21

 PURPOSE.....21

 SCOPE.....21

 PERSONAL RESPONSIBILITY.....21

 NATIONAL AUTHORITIES FOR SECURITY MATTERS21

 President of the United States.....21

 National Security Council (NSC).....21

 DNI.....21

 ISOO.....22

 CUI Office (CUIO).....22

 DoD INFORMATION SECURITY PROGRAM MANAGEMENT.....22

 USD(I).....22

 USD(P).....22

 DoD CIO.....22

 National Security Agency/Central Security Service (NSA/CSS).....23

 DIA.....23

 Defense Security Service (DSS).....23

 DTIC.....23

 DoD Joint Referral Center (JRC).....23

 DoD COMPONENT INFORMATION SECURITY MANAGEMENT23

 Head of the DoD Component23

 Senior Agency Officials.....24

 Activity Security Management24

 TSCO25

 Other Security Management Roles25

USE OF CONTRACTORS IN SECURITY ADMINISTRATION	26
CLASSIFICATION AUTHORITY	27
CLASSIFICATION POLICY	27
RECLASSIFICATION	27
ACCESS TO CLASSIFIED INFORMATION	28
Requirements for Access	28
Nondisclosure Agreements	28
NATO Briefing for Cleared Personnel	28
Access By Individuals Outside the Executive Branch.....	29
PROTECTION REQUIREMENTS.....	29
Protection of Restricted Data (RD) and Formerly Restricted Data (FRD).....	29
Protection of SCI.....	30
Protection of COMSEC Information	30
Protection of SAP Information	30
Protection of NATO and FGI	30
Protection of Nuclear Command and Control-Extremely Sensitive Information (NC2-ESI).....	30
RETENTION	30
PERMANENTLY VALUABLE RECORDS.....	30
MILITARY OPERATIONS	31
WAIVERS	31
CORRECTIVE ACTIONS AND SANCTIONS	31
Procedures.....	31
Sanctions.....	31
Reporting of Incidents.....	32
ENCLOSURE 4: CLASSIFYING INFORMATION.....	33
CLASSIFICATION POLICY.....	33
CLASSIFICATION PROHIBITIONS	33
LEVELS OF CLASSIFICATION	34
Top Secret	34
Secret.....	34
Confidential.....	34
ORIGINAL CLASSIFICATION.....	34
REQUESTS FOR OCA	35
ORIGINAL CLASSIFICATION PROCESS	36
CHANGING THE LEVEL OF CLASSIFICATION	37
SECURITY CLASSIFICATION GUIDANCE.....	38
TENTATIVE CLASSIFICATION.....	38
DERIVATIVE CLASSIFICATION.....	38
RESPONSIBILITIES OF DERIVATIVE CLASSIFIERS	39
PROCEDURES FOR DERIVATIVE CLASSIFICATION	39
DURATION OF CLASSIFICATION	40
Originally Classified Information.....	40
Derivatively Classified Information	41

Extending the Duration of Classification.....41

FORMAT FOR DISSEMINATION.....41

COMPILATIONS.....41

CLASSIFICATION OF ACQUISITION INFORMATION43

CLASSIFICATION OF INFORMATION RELEASED TO THE PUBLIC43

 Classified Information Released Without Proper Authority.....43

 Reclassification of Information Declassified and Released to the Public Under
 Proper Authority44

 Information Declassified and Released to the Public Without Proper Authority.....46

CLASSIFICATION OR RECLASSIFICATION FOLLOWING RECEIPT OF A
REQUEST FOR INFORMATION.....46

CLASSIFYING NON-GOVERNMENT RESEARCH AND DEVELOPMENT
INFORMATION.....47

THE PATENT SECRECY ACT OF 195247

REQUESTS FOR CLASSIFICATION DETERMINATION48

CHALLENGES TO CLASSIFICATION.....49

 Principles.....49

 Procedures.....49

ENCLOSURE 5: DECLASSIFICATION AND CHANGES IN CLASSIFICATION.....51

 DECLASSIFICATION POLICY51

 PROCESSES FOR DECLASSIFICATION52

 AUTHORITY TO DECLASSIFY52

 DECLASSIFICATION GUIDANCE.....53

 DECLASSIFICATION OF INFORMATION.....53

 CANCELING OR CHANGING CLASSIFICATION MARKINGS.....54

 SPECIAL PROCEDURES FOR CRYPTOLOGIC INFORMATION.....54

 PERMANENTLY VALUABLE RECORDS.....54

 RECORDS DETERMINED NOT TO HAVE PERMANENT HISTORICAL VALUE.....55

 EXTENDING CLASSIFICATION BEYOND 25 YEARS FOR UNSCHEDULED
 RECORDS55

 CLASSIFIED INFORMATION IN THE CUSTODY OF CONTRACTORS,
 LICENSEES, GRANTEES, OR OTHER AUTHORIZED PRIVATE
 ORGANIZATIONS OR INDIVIDUALS55

 AUTOMATIC DECLASSIFICATION.....55

 Deadline56

 Secretary of Defense Certification.....56

 Public Release of Automatically Declassified Documents.....56

 Basis for Exclusion or Exemption from Automatic Declassification.....56

 Exclusion of RD and FRD57

 Integral File Block57

 Delays of Automatic Declassification57

 Automatic Declassification of Backlogged Records at NARA59

 Declassification Review Techniques59

 EXEMPTIONS FROM AUTOMATIC DECLASSIFICATION59

Exemption Types	59
Exemption Criteria and Duration	60
Exemption Requests.....	62
When to Request an Exemption.....	63
Who Identifies and Requests an Exemption	63
ISCAP Authority.....	63
Notice to Information Holders	63
DECLASSIFICATION OF INFORMATION MARKED WITH OLD DECLASSIFICATION INSTRUCTIONS.....	64
REFERRALS IN THE AUTOMATIC DECLASSIFICATION PROCESS.....	64
Description.....	64
Referral Responsibility	64
MANDATORY DECLASSIFICATION REVIEW	64
SYSTEMATIC REVIEW FOR DECLASSIFICATION	67
DOWNGRADING CLASSIFIED INFORMATION.....	67
UPGRADING CLASSIFIED INFORMATION	67
DECLASSIFYING FGI.....	68
APPLICATION OF DECLASSIFICATION AND EXTENSION OF CLASSIFICATION TO PRESENT AND PREDECESSOR EXECUTIVE ORDERS	68
ENCLOSURE 6: SECURITY CLASSIFICATION GUIDES	69
GENERAL.....	69
CONTENT OF SECURITY CLASSIFICATION GUIDES	69
CUI AND UNCLASSIFIED ELEMENTS OF INFORMATION.....	70
DATA COMPILATION CONSIDERATIONS	70
APPROVAL OF SECURITY CLASSIFICATION GUIDES.....	71
DISTRIBUTION OF SECURITY CLASSIFICATION GUIDES.....	71
INDEX OF SECURITY CLASSIFICATION GUIDES	72
REVIEW OF SECURITY CLASSIFICATION GUIDES	72
REVISION OF SECURITY CLASSIFICATION GUIDES	72
CANCELLING SECURITY CLASSIFICATION GUIDES	72
REPORTING CHANGES TO SECURITY CLASSIFICATION GUIDES	73
FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEWS	73
GLOSSARY	74
PART I. ABBREVIATIONS AND ACRONYMS	74
PART II. DEFINITIONS.....	75
FIGURES	
1. Patent Secrecy Act Statement	48
2. Patent Secrecy Act Foreign Registration Statement	48

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (b) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive
Compartmented Information," October 9, 2008
- (c) DoD 5200.1-R, "Information Security Program," January 14, 1997 (hereby cancelled)
- (d) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (e) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
- (f) Part 2001 of title 32, Code of Federal Regulations
- (g) DoD O-5200.1-I, "Index of Security Classification Guides (U)," September 1, 1996 (hereby
cancelled)
- (h) Directive-Type Memorandum 04-010, "Interim Information Security Guidance," April 16,
2004 (hereby cancelled)
- (i) Directive-Type Memorandum 11-004, "Immediate Implementation Provisions of Executive
Order 13526, 'Classified National Security Information,'" April 26, 2011 (hereby
cancelled)
- (j) DoD 5105.21-M-1, "Department of Defense Sensitive Compartmented Information
Administrative Security Manual," August 1998
- (k) DoD 8910.1-M, "Department of Defense Procedures for Management of Information
Requirements," June 30, 1998
- (l) Section 2723 of title 10, United States Code
- (m) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P)),
December 8, 1999
- (n) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
- (o) DoD 5200.2-R, "Personnel Security Program," January 1987
- (p) DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty
Organization Affairs (USSAN)," February 27, 2006
- (q) United States Security Authority for NATO Affairs Instruction 1-07, "Implementation of
North Atlantic Treaty Organization (NATO) Security Requirements," April 5, 2007¹
- (r) DoD Directive 5230.09, "Clearance of DoD Information for Public Release,"
August 22, 2008
- (s) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public
Release," January 8, 2009
- (t) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 7,
1998, with attached "Web Site Administration Policies and Procedures," November 25,
1998
- (u) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign
Governments and International Organizations," June 16, 1992
- (v) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (w) DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD
Physical Security Review Board (PSRB)," December 10, 2005

¹ Available from the Central U.S. Registry.

- (x) DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985
- (y) Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended
- (z) Director of Central Intelligence Directive 6/1, "Security Policy for Sensitive Compartmented Information and Security Policy Manual," March 1, 1995²
- (aa) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (ab) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (ac) Sections 402, 431, 432, 432a, 432b, 1801(p) and 2673 of title 50, United States Code
- (ad) Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," January 20, 2004
- (ae) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
- (af) Part 1045 of title 10, Code of Federal Regulations
- (ag) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
- (ah) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information," July 5, 1990³
- (ai) DoD Instruction 3305.13, "DoD Security Training," December 18, 2007
- (aj) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
- (ak) National Security Agency/Central Security Service Policy Manual 3-16, "Control of Communications Security (COMSEC) Material," August 5, 2005⁴
- (al) DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12, 2010
- (am) Office of Management and Budget Circular No. A-76, "Performance of Commercial Activities," May 29, 2003, as revised
- (an) Section 2011, et seq, of title 42, United States Code (also known as "The Atomic Energy Act of 1954, as amended")
- (ao) DoD Directive 5210.48, "Polygraph and Credibility Assessment Program," January 25, 2007
- (ap) DoD Instruction 5210.02, "Access to and Dissemination of Restricted Data and Formerly Restricted Data," June 3, 2011
- (aq) DoD Instruction O-5205.11, "Management, Administration, Oversight of DoD Special Access Programs (SAPs)," July 1, 1997
- (ar) Chairman of the Joint Chiefs of Staff Instruction 3231.01B, "Safeguarding Nuclear Command and Control Extremely Sensitive Information," June 21, 2006⁵
- (as) Chapters 21, 22,⁶ 31, 33, and 35 of title 44, United States Code
- (at) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
- (au) Sections 801-940 of title 10, United States Code (also known as "The Uniform Code of Military Justice")
- (av) Sections 102, 105, 552,⁷ and 552a⁸ of title 5, United States Code

² Available from the Office of the Director of National Intelligence.

³ Available on SIPRNET at http://www.iad.nsa.smil.mil/resources/library/natl_pols_dirs_orders_section/index.cfm.

⁴ For Official Use Only document, available to authorized users. Contact the NSA/CSS Office of Corporate Policy (DJP1) for assistance.

⁵ This document is For Official Use Only. It is available to authorized recipients at https://ca.dtic.mil/cjcs_directives/index.htm

⁶ Chapter 22 is also known as "The Presidential Records Act of 1978."

- (aw) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003
- (ax) DoD Instruction 5000.02, “Operation of the Defense Acquisition System,” December 8, 2008
- (ay) DoD Instruction 5200.39, “Critical Program Information (CPI) Protection Within the Department of Defense,” July 16, 2008
- (az) DoD Directive 3204.1, “Independent Research and Development (IR&D) and Bid and Proposal (B&P) Program,” May 10, 1999
- (ba) Sections 181 through 188 of title 35, United States Code (also known as “The Patent Secrecy Act of 1952”)
- (bb) DoD Directive 5230.25, “Withholding of Unclassified Technical Data From Public Disclosure,” November 6, 1984
- (bc) Public Law 106-65, “National Defense Authorization Act for Fiscal Year 2000,” October 5, 1999
- (bd) Section 3161 of Public Law 105-261, “Strom Thurmond National Defense Authorization Act for Fiscal Year 1999,” October 17, 1998, as amended (also known as “The Kyl-Lott Amendment”)
- (be) Presidential Memorandum, “Implementation of the Executive Order, ‘Classified National Security Information,’” December 29, 2009
- (bf) Executive Order 12951, “Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems,” February 22, 1995
- (bg) DoD 7000.14-R, Volume 11A, “Department of Defense Financial Management Regulation: Reimbursable Operations, Policy and Procedures,” May 2001
- (bh) DoD Directive 3200.12, “DoD Scientific and Technical Information (STI) Program (STIP),” February 11, 1998
- (bi) Executive Order 12958, “Classified National Security Information,” April 20, 1995, as amended
- (bj) DoD 5200.1-H, “Department of Defense Handbook For Writing Security Classification Guidance,” November 1999
- (bk) DoD 5400.7-R, “DoD Freedom of Information Act Program,” September 4, 1998

⁷ Section 552 is also known as “The Freedom of Information Act.”

⁸ Section 552a is also known as “The Privacy Act of 1974, as amended.”

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall:

a. Serve as the DoD Senior Security Official, in accordance with Reference (a), and in that capacity shall be the DoD Senior Agency Official appointed pursuant to subsection 5.4(d) of Reference (d) to direct, administer, and oversee the DoD Information Security Program.

b. Notify the Congress and the Director, Information Security Oversight Office (ISOO), as appropriate, of violations involving classified information and of approval of waivers involving Reference (d) and its implementing directive (Reference (f)), as required by section 2723 of title 10, United States Code (U.S.C.) (Reference (l)) and References (d) and (f).

c. Establish requirements for collecting and reporting data as necessary to fulfill the requirements of References (d) and (f) and other national-level guidance.

d. Designate a senior-level Federal employee, and an alternate, to represent the Department of Defense on the Interagency Security Classification Appeals Panel (ISCAP) as required by Reference (d). The individuals so designated must be full-time or permanent part-time employees of the Department of Defense. Designate to the ISCAP Chair in writing one or more individuals as identified by the Director, Washington Headquarters Services (WHS) to serve as a liaison in support of the DoD representative in accordance with the ISCAP bylaws in Reference (f).

e. Determine investigative responsibility for unauthorized disclosures and damage assessments in consultation with the affected DoD Components when responsibility is unclear or is shared among DoD Components and serve as the principal point of contact on counterintelligence (CI) and security investigative matters that involve the unauthorized disclosure of classified information directed to the Department of Defense by other U.S. Government agencies or that may involve other U.S. Government agencies.

2. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall:

a. Serve as the senior official responsible for administering that portion of the DoD Information Security Program pertaining to the National Classified Military Information Disclosure Policy, foreign government (including North Atlantic Treaty Organization (NATO)) information, and security arrangements for international programs in accordance with DoDD 5111.1 (Reference (m)) and Reference (a).

b. Notify the Director, ISOO, of approval of waivers involving Reference (d) and its implementing directive (Reference (f)).

3. DoD CHIEF INFORMATION OFFICER (CIO). The DoD CIO shall:

a. Establish procedures, consistent with References (d) and (f) and this Manual, to ensure that information systems, including networks and telecommunications systems, that process, disseminate, or store classified information:

(1) Prevent access by unauthorized persons.

(2) Assure the integrity of the information.

(3) Use, to the maximum extent practicable, common information technology (IT) standards, protocols, and interfaces, and standardized electronic formats to maximize availability and authorized access.

b. Direct the use of technical means to prevent unauthorized copying of classified data and for anomaly detection to recognize unusual patterns of accessing, handling, downloading, and removal of digital classified information.

4. ADMINISTRATOR, DEFENSE TECHNICAL INFORMATION CENTER (DTIC). The Administrator, DTIC, under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics and in addition to the responsibilities in section 6 of this enclosure, shall maintain an index of security classification guides in an online database accessible through www.dtic.mil.

5. DIRECTOR, WHS. The Director, WHS, under the authority, direction, and control of the Director, Administration and Management, shall identify to the USD(I) an individual and at least one alternate to serve as the ISCAP liaison for the Department of Defense in accordance with the ISCAP Bylaws in Reference (f).

6. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall, in accordance with Reference (b):

a. Be responsible for the overall management, functioning, and effectiveness of the information security program within their respective DoD Component.

b. Appoint a senior agency official to be responsible for directing, administering, and overseeing the information security program within the Component on his or her behalf and ensure that official accomplishes the responsibilities in section 7 of this enclosure. The DoD Component Head may designate a separate senior official to be responsible for overseeing SAPs within the Component, if necessary, in accordance with DoDD 5205.07 (Reference (n)).

c. If the Component is not an element of the Intelligence Community, designate a senior intelligence official to be responsible for ensuring adequate funding and effective

implementation of the Component's SCI security program, including awareness and education, consistent with guidance established by the DNI.

d. Identify, program for, and commit necessary resources to effectively implement the requirements for protection of classified information as part of the Component's information security program.

e. Conduct, as periodically directed by the USD(I), reviews of the DoD Component's classification guidance and provide reports summarizing results.

f. Ensure the Component Senior Agency Official and the Component Senior Intelligence Official coordinate as appropriate to achieve a harmonized and cohesive information security program within the DoD Component.

7. SENIOR AGENCY OFFICIALS. The senior agency officials, under the authority, direction, and control of the Heads of the DoD Components, appointed in accordance with section 6 of this enclosure shall, in addition to the responsibilities in Volume 4 of this Manual:

a. Direct, administer, and oversee their respective DoD Component's information security program.

b. Develop guidance as necessary for program implementation within the DoD Component.

c. Direct the head of each activity within the DoD Component that creates, handles, or stores classified information to appoint, in writing, an official to serve as security manager for the activity, to properly manage and oversee the activity's information security program. Persons appointed to these positions shall be provided training as Enclosure 5 of Volume 3 of this Manual requires.

d. Establish and maintain an ongoing self-inspection and oversight program to evaluate and assess the effectiveness and efficiency of the DoD Component's implementation of that portion of the information security program pertaining to classified information.

(1) Evaluation criteria shall consider, at a minimum, original and derivative classification, declassification, safeguarding, security violations, education and training, and management and oversight.

(2) The program shall include regular review and assessment of representative samples of the DoD Component's classified products. Appropriate officials shall be authorized to correct misclassification of information, except for information covered by paragraph 17.b. or section 18 of Enclosure 4 of this Volume.

(3) Self-inspections shall be conducted at least annually with the frequency established based on program needs and classification activity. DoD Component activities that originate significant amounts of classified information should be inspected at least annually. Annual

reports on the Component's self-inspection program shall be submitted as required by ISOO and/or USD(I). The report shall include:

(a) A description of the agency's self inspection program, to include activities assessed, program areas covered, and methodology utilized.

(b) A summary of the findings in the following program areas: original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight.

(c) Specific information on the findings of the annual review of agency original and derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies that were identified.

(d) Actions taken or planned to correct identified deficiencies or misclassification actions, and to deter their recurrence.

(e) Best practices identified.

e. Establish procedures to prevent unauthorized persons from accessing classified information, including:

(1) Specific requirements for protecting classified information at DoD Component-sponsored meetings and conferences, to include seminars, exhibits, symposiums, conventions, training activities, workshops, or other such gatherings, during which classified information is disseminated.

(2) Requirements for protecting U.S. classified information located in foreign countries, with particular attention on ensuring proper enforcement of controls on release of U.S. classified information to foreign entities.

(3) Procedures to accommodate visits to DoD Component facilities involving access to, or disclosure of, classified information.

f. Establish and maintain declassification programs and plans that meet the requirements of this Manual and ensure that necessary resources are applied to the review of information to ensure it is neither classified for longer than necessary nor declassified prematurely.

g. Establish and maintain a security education and training program as required by Enclosure 5 of Volume 3 of this Manual, ensure that DoD Component personnel receive security education and training as appropriate to their functions, and grant, when appropriate, waivers to the original and derivative classification training requirements of section 7 of Enclosure 5 of Volume 3.

h. Ensure that the performance contract or other system used to rate the performance of civilian and military personnel includes the designation and management of classified

information, to include Restricted Data and Formerly Restricted Data information when appropriate, as a critical element or item to be evaluated in the rating of:

- (1) Original classification authorities.
- (2) Security managers and security specialists.
- (3) Personnel who derivatively classify information on a routine basis.
- (4) Information system security personnel if their duties involve access to classified information and information system personnel (e.g., system administrators) with privileged access to classified system or network resources.
- (5) All other personnel whose duties include significant involvement with the creation or handling of classified information.
 - i. Account for the costs associated with implementing this Manual within the DoD Component and report those costs as required.
 - j. Ensure prompt and appropriate response to any request, appeal, challenge, complaint, or suggestion arising out of implementation of this Manual within the DoD Component.
 - k. Establish procedures for receipt of information, allegations, or complaints regarding over-classification or incorrect classification within the DoD Component and, as needed, provide guidance to personnel on proper classification.
 - l. Approve, when appropriate, the use of alternative compensatory control measures (ACCM) for classified information over which the senior agency official has cognizance and provide written notification within 30 days to the Director of Security, Office of the Under Secretary of Defense for Intelligence (OUSD(I)), or the Director, International Security Programs, Defense Technology Security Administration, Office of the USD(P) (OUSD(P)), as appropriate, when establishing or terminating an ACCM.
 - m. Submit an annual report addressing how the DoD Component implemented that portion of the information security program dealing with classified information.
 - (1) The report, covering the previous fiscal year, shall be submitted on Standard Form (SF) 311, "Agency Information Security Program Data," to reach the Director of Security, OUSD(I), prior to October 31 of each year. The Military Departments shall submit their reports directly to ISOO, with a copy furnished to OUSD(I). OUSD(I) shall compile the reports, excluding those of the Military Departments, and provide a consolidated report to ISOO.
 - (2) The SF 311 shall be completed according to the instructions accompanying the form and those provided by ISOO and OUSD(I).
 - n. Submit to the Director of Security, OUSD(I), prior to October 31 of each year, a report

listing, by position title, those officials within the DoD Component who hold original classification authority (OCA) delegated in accordance with paragraph 4.c. of Enclosure 4 and those officials who hold declassification authority delegated in accordance with paragraph 3.b. of Enclosure 5. The report shall be organized by level of highest classification authority and by activity.

o. Cooperate and coordinate with the Component senior intelligence official as appropriate to achieve a harmonized and cohesive information security program within the DoD Component.

8. HEADS OF DoD ACTIVITIES. The heads of DoD activities shall:

a. Be responsible for overall management, functioning and effectiveness of the activity's information security program.

b. Designate, in writing, an activity security manager, who shall be given the necessary authority to ensure personnel adhere to program requirements. Provide the designated activity security manager direct access to activity leadership and ensure he or she is organizationally aligned to ensure prompt and appropriate attention to program requirements.

(1) The activity security manager may be assigned full-time, part-time, or as a collateral duty, provided that the responsibilities delineated in section 9 of this enclosure can be adequately and professionally executed and implemented.

(2) The activity security manager shall:

(a) Be a military officer, senior non-commissioned officer, or a civilian employee with sufficient authority, staff, and other resources necessary to manage the program for the activity.

1. For activities with more than 100 personnel assigned, a senior non-commissioned officer designated as the activity security manager shall be E-7 or above; a civilian employee so designated shall be GS-11 or above (or pay band equivalent).

2. For activities with less than 100 personnel assigned, a senior non-commissioned officer designated as the activity security manager shall be E-6 or above; a civilian employee so designated shall be GS-7 or above (or pay band equivalent).

(b) Be a U.S. citizen.

(c) Have been the subject of a favorably adjudicated, current background investigation appropriate for the highest level of classification of information handled by personnel within the activity in accordance with requirements of DoD 5200.2-R (Reference (o)).

(d) Have access appropriate to the level of information managed.

c. In large activities and where circumstances warrant, designate, in writing, activity assistant security manager(s) to assist in program implementation, maintenance, and local oversight.

(1) Responsibilities assigned to assistant security managers shall be commensurate with their grade level, experience, and training.

(2) Individuals assigned as assistant security managers shall be U.S. citizens with security clearances and accesses appropriate to their assigned responsibilities.

(3) Assistant security managers shall report directly to the activity security manager who shall provide guidance, direction, coordination, training, and oversight necessary to ensure that the program is being administered effectively.

d. Optionally, where circumstances warrant (such as in activities with large repositories of Top Secret information), designate an activity Top Secret control officer (TSCO) to manage and account for Top Secret materials, and Top Secret control assistant(s) (TSCA(s)) as needed to assist the TSCO. When used, designations shall be in writing. Top Secret couriers are NOT considered TSCA(s).

(1) An individual designated as the TSCO must have been the subject of a favorably adjudicated, current background investigation in accordance with requirements of Reference (o) and must have Top Secret access. The TSCO shall report directly to the activity security manager, or the activity security manager may serve concurrently as the TSCO.

(2) An individual designated as a TSCA must have been the subject of a favorably adjudicated, current background investigation in accordance with requirements of Reference (o) and must have Top Secret access.

e. When required by DoDD 5100.55 (Reference (p)), designate, in writing, an activity NATO control point officer and at least one alternate to ensure that NATO information is correctly controlled and accounted for, and that NATO security procedures are followed. NATO Instruction 1-07 (Reference (q)) establishes procedures and minimum security standards for the handling and protection of NATO classified information.

9. ACTIVITY SECURITY MANAGER. The activity security manager shall:

a. Manage and implement the DoD activity's information security program on behalf of the activity head, to whom he or she shall have direct access.

b. Serve as the principal advisor and representative to the activity head in all matters pertaining to this Manual and maintain cognizance of all activity information, personnel, information systems, physical and industrial security functions to ensure that the information security program is coordinated in its execution and inclusive of all requirements in this Manual.

c. Provide guidance, direction, coordination, and oversight to designated assistant security managers, TSCOs, TSCAs, security assistants and, as appropriate, others in security management roles as necessary to ensure that all elements of the information security program are being administered effectively, efficiently, and in a coordinated manner.

d. Develop a written activity security instruction that shall include provisions for safeguarding classified information during emergency situations and military operations, if appropriate.

e. Ensure that personnel in the activity who perform security duties are kept abreast of changes in policies and procedures, and provide assistance in problem solving.

f. Formulate, coordinate, and conduct the activity security education and training program. Organizations with elements that are deployable for contingency operations shall ensure information security training, to include appropriate application to information systems, is an integral part of predeployment training and preparation.

g. Ensure that threats to security and security incidents pertaining to classified information, including foreign government information (FGI), are reported, recorded, coordinated with the proper authorities, and, when necessary, investigated and that appropriate action is taken to mitigate damage and prevent recurrence. Ensure that incidents involving the loss or compromise of classified material (as described in Enclosure 6 of Volume 3 of this Manual) are immediately referred to the cognizant investigative authority. In cases where compromise is determined or cannot be ruled out, ensure that security reviews and other required assessments are conducted as soon as possible. Coordinate with local information assurance officials, but retain responsibility for inquiries into incidents involving possible or actual compromise of classified information resident in or on IT systems.

h. Coordinate the preparation, dissemination, and maintenance of security classification guides under the activity's cognizance as required by Enclosure 6 of this Volume.

i. Maintain liaison with the activity public affairs officer or information security officer, as appropriate, and the operations security (OPSEC) officer to ensure that information, including press releases and photos, proposed or intended for public release, including via website posting, is subject to a security review in accordance with DoDD 5230.09 (Reference (r)), DoDI 5230.29 (Reference (s)), and Deputy Secretary of Defense Memorandum (Reference (t)).

j. Coordinate with other activity officials regarding security measures for the classification, safeguarding, transmission, declassification, and destruction of classified information.

(1) Coordinate as required with the foreign disclosure officer on all matters governing the disclosure of classified information to foreign governments and international organizations in accordance with DoDD 5230.11 (Reference (u)).

(2) Ensure implementation of and compliance with the requirements of this Manual for all uses of IT. Coordinate with information systems security personnel (e.g., designated approval

authorities (DAAs), information assurance managers (IAMs), information system security managers) as required for effective management, use, and oversight of classified information in electronic form.

k. Develop security measures and procedures, consistent with DoDD 5230.20 (Reference (v)), DoDI 5200.08 (Reference (w)) and other applicable policies, regarding visitors who require access to classified information and facilities containing same.

l. Ensure compliance with the requirements of this Manual when access to classified information is provided to industry at activity facilities and locations in connection with a classified contract. If the classified information is provided to industry at the contractor's facility, ensure compliance with the provisions of DoD 5220.22-R (Reference (x)).

m. Ensure that access to classified information is limited to appropriately cleared personnel with a need to know as required by section 4.1 of Reference (d) and section 3.1 of E.O. 12968 (Reference (y)).

n. Maintain liaison with the special security officer (SSO), as appropriate, on issues of common concern.

10. TSCO. The TSCO, when designated in accordance with paragraph 8.d. of this enclosure, shall:

a. For paper documents and other physical media (e.g., disk drives and removable computer media), maintain a system of accountability (e.g., registry) to record the receipt, reproduction, transfer, transmission, downgrading, declassification, and destruction of Top Secret information, less SAP, SCI, and other special types of classified information.

b. Ensure that inventories of Top Secret information are conducted at least annually or more frequently when circumstances warrant.

11. SENIOR INTELLIGENCE OFFICIALS. The senior intelligence officials, including those who are heads of elements of the Intelligence Community and those designated according to paragraph 6.c of this enclosure, shall:

a. In accordance with Reference (b):

(1) Protect intelligence and intelligence sources and methods from unauthorized disclosure consistent with the policies of the DNI and, where applicable, the requirements of this Manual and Reference (j).

(2) Administer and oversee, within their respective organizations, those aspects of the SCI security programs not delegated to Defense Intelligence Agency (DIA) in accordance with Reference (b).

(3) Develop DoD Component-specific implementation guidance as necessary for the protection of SCI.

b. Cooperate and coordinate with the Component senior agency official as appropriate to achieve a harmonized and cohesive information security program within the DoD Component.

c. Where required by this Manual, provide the USD(I) with copies of requests for exceptions and waivers of information security policies, security incident reports, and other information submitted to the DNI.

d. Designate, as required by Director of Central Intelligence Directive 6/1 (Reference (z)) and Reference (j), an activity SSO to be responsible for the day-to-day security management, operation, implementation, use, and dissemination of SCI within the activity and, as needed, alternate SSO(s). Such designations shall be made for any activity that is accredited for and authorized to receive, use, and store SCI and shall be in writing.

(1) All SCI matters shall be referred to the SSO.

(2) The SSO may be designated as the activity security manager if the grade requirements for the position are met; however, the activity security manager cannot function as the SSO unless so designated by the cognizant senior intelligence official.

12. INFORMATION SYSTEMS SECURITY OFFICIALS. Information systems security officials (e.g., DAA, IAM, information assurance officer) designated, in writing, as required by DoDD 8500.01E (Reference (aa)) and DoDI 8500.2 (Reference (ab)), shall:

a. Coordinate with the activity security manager regarding implementation of information systems security measures and procedures.

b. Notify the activity security manager, who retains overall security responsibility for required inquiries and investigations, when there are incidents involving possible or actual compromise or data spills of classified information resident in information systems, as required by Reference (ab), and coordinate with him or her as required for resolution of the incident.

ENCLOSURE 3

DoD INFORMATION SECURITY PROGRAM OVERVIEW

1. PURPOSE. Effective execution of a robust information security program that gives equal priority to both protecting information and demonstrating a commitment to open Government and that includes accurate, accountable application of classification standards and routine, secure, and effective declassification is a national security imperative. This Manual provides overarching program guidance and direction for the DoD Information Security Program. While day-to-day program execution is the responsibility of all DoD personnel, program implementation must be guided by active and engaged senior managers at all levels who have the responsibility for overall program execution and by security managers who ensure the program is visible, effective, and efficient.

2. SCOPE. The DoD Information Security Program implements References (b), (d), and (f) with regard to the classification, declassification, and protection of classified information, including information categorized as collateral, SCI, and SAP, and provides guidance to users to identify, mark, and protect certain types of unclassified information, referred to as CUI, in accordance with Reference (e) and other national-level directives. This combined guidance is known as the DoD Information Security Program and is applicable to all DoD Components.

3. PERSONAL RESPONSIBILITY. All personnel of the Department of Defense are personally and individually responsible for properly protecting classified information and CUI under their custody and control. All officials within the Department of Defense who hold command, management, or supervisory positions have specific, non-delegable responsibility for the quality and effectiveness of implementation and management of the information security program within their areas of responsibility.

4. NATIONAL AUTHORITIES FOR SECURITY MATTERS

a. President of the United States. The President of the United States bears executive responsibility for the security of the Nation, which includes the authority to classify information for the protection of the national defense and foreign relations of the United States. The President has established standards for the classification, safeguarding, and declassification of national security information through the issuance of Reference (d) and for the designation and protection of CUI through the issuance of Reference (e).

b. National Security Council (NSC). In accordance with section 402 of title 50, U.S.C. (Reference (ac)), the NSC provides overall policy guidance on information security.

c. DNI. The DNI is head of the Intelligence Community and principal advisor to the President and the NSC for intelligence matters related to national security pursuant to Section

1011 of Public Law 108-458 (Reference (ad)) and Section 1.3 of E.O. 12333 (Reference (ae)). The DNI is also charged by section 1.3 (b)(8) of Reference (ae) with protecting intelligence sources, methods, and activities, and in this role, the DNI issues instructions in the form of Intelligence Community Directives or other security policies and standards for the protection, management and oversight of SCI and other national intelligence.

d. ISOO. The ISOO, under the authority of the Archivist of the United States, acting in consultation with the NSC, issues directives as necessary to implement Reference (d). The directives establish national standards for the classification and marking of national security information, security education and training programs, safeguarding, self-inspection programs, and declassification. The ISOO has the responsibility to oversee agency implementation and compliance with these directives. In this role, the ISOO requests certain information regarding DoD activities, and such requests are coordinated through USD(I).

e. CUI Office (CUIO). The CUIO, under the authority of the Archivist of the United States, issues directives as necessary to implement Reference (e). The directives establish national standards for designation, safeguarding, marking, and dissemination of CUI as well as standards for education and training. The CUIO has the responsibility to oversee agency implementation and compliance with these directives. CUIO requests for information regarding DoD activities are coordinated through USD(I).

5. DoD INFORMATION SECURITY PROGRAM MANAGEMENT

a. USD(I). Reference (a) designates the USD(I) as the DoD Senior Security Official. In this role, the USD(I) is the DoD Senior Agency Official responsible for directing, administering, and overseeing the DoD Information Security Program for the Department of Defense, and except as provided in paragraph 5.b. of this section, performs the functions specified in subsection 5.4(d) of Reference (d) and its implementing directives for the Department of Defense. The USD(I) is also the Restricted Data Management Official for the Department of Defense in accordance with part 1045 of title 10, Code of Federal Regulations (Reference (af)).

b. USD(P). In accordance with Reference (m), the USD(P) is the senior official responsible for directing, administering, and overseeing that portion of the DoD Information Security Program pertaining to foreign government (including NATO) information, the disclosure of classified information to foreign governments and international organizations, and security arrangements for international programs. Within the scope of these responsibilities, the USD(P) also performs the functions specified in subsection 5.4(d) of Reference (d) and its implementing directives for the Department of Defense.

c. DoD CIO. In accordance with DoDD 5144.1 (Reference (ag)), the DoD CIO is responsible for assuring the confidentiality, authentication, integrity, availability, and non-repudiation of DoD IT systems and the networks that connect them. These functions are collectively referred to as information assurance (IA).

d. National Security Agency/Central Security Service (NSA/CSS). In accordance with Reference (ae), the NSA/CSS provides centralized coordination and direction for signals intelligence. In accordance with National Security Directive 42 (Reference (ah)), the NSA/CSS provides IA support for national security systems and vulnerability assessments at the request of the national security system owner. Additionally, in accordance with Reference (b), the Director, NSA/Chief, CSS may impose special requirements for protection of classified cryptologic information.

e. DIA. As assigned by Reference (b) and with the exception of NSA/CSS, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency, DIA administers within the Department of Defense the SCI security policies and procedures issued by the DNI. The Director, DIA, is responsible for development of standards, implementation, and operational management of the SCI compartments for the Department of Defense.

f. Defense Security Service (DSS). DSS provides information security education and training for the Department of Defense as required by DoDI 3305.13 (Reference (ai)). DSS, as the DoD cognizant security office for industrial security, also manages and administers the DoD portion of the National Industrial Security Program, to ensure the protection of classified information released or disclosed to industry in connection with classified contracts.

g. DTIC. DTIC maintains a repository and index of security classification guides, as specified in paragraph 6.c of Enclosure 6 of this Volume, for the Department of Defense. DTIC also administers and controls secondary release and dissemination of technical documents and data, including production, engineering, and logistics information, marked with the distribution statements required by DoDD 5230.24 (Reference (aj)). Such citations serve as the authoritative record for controlling office classification and distribution decisions for the documents in the DTIC collections.

h. DoD Joint Referral Center (JRC). In accordance with Reference (b), the JRC serves as an adjunct to the National Declassification Center (NDC), established by Reference (d), for processing internal and external referrals of documents containing defense information as part of the declassification process for records determined to have permanent historical value. The JRC is a joint DoD Component operation co-located with the Army Declassification Activity. The JRC is tasked to streamline declassification processes, facilitate quality assurance measures, and implement standardized training consistent with those of the NDC. DoD Component declassification activities shall continue to conduct initial reviews of records eligible for automatic declassification in accordance with the Volume until the NDC issues implementing instructions.

6. DoD COMPONENT INFORMATION SECURITY MANAGEMENT

a. Head of the DoD Component. The Head of each DoD Component has overall responsibility for implementation of the information security program within the Component. This includes responsibility for:

(1) Designating senior agency officials, including, as appropriate, the DoD Component senior agency official and senior intelligence official, to be responsible for directing, administering, and overseeing the information security program within the Component. A separate senior official responsible for overseeing SAPs within the Component may also be designated.

(2) Committing necessary resources to effectively implement the information security program.

b. Senior Agency Officials. The senior agency official appointed by the Head of the DoD Component has day-to-day responsibility for the direction, implementation, and oversight of Component's information security program and for its efficient and effective implementation. These responsibilities include:

(1) Promulgating guidance necessary for program implementation.

(2) Ensuring adequate resources for a robust information security program are identified and programmed.

(3) Establishing and maintaining a security education program.

(4) Establishing and maintaining an ongoing self-inspection and program oversight function.

(5) Directing the head of each activity within the DoD Component that creates, handles, or stores classified information to appoint an official to serve as security manager for the activity, to properly manage and oversee the activity's information security program.

c. Activity Security Management. The activity security manager manages and implements the activity's information security program and ensures its visibility and effectiveness on behalf of the activity head, who retains the responsibility for overall management and functioning of the program. The activity security managers must have sufficient delegated authority to ensure that personnel adhere to program requirements, and their position within the organizational hierarchy must ensure their credibility and enable them to raise security issues directly to their respective activity head.

(1) Some tasks may be assigned to a number of activity personnel and may even be assigned to persons senior to the security manager. Nevertheless, the security manager shall remain cognizant of all activity information, personnel, information systems, and physical and industrial security functions, and shall ensure that the information security program is coordinated and inclusive of all requirements in this Manual.

(2) The activity security manager responsibilities include:

(a) Serving as the principal advisor and representative to the activity head in all matters pertaining to this Manual.

- (b) Developing a written activity security instruction.
- (c) Ensuring that personnel in the activity who perform security duties are trained.
- (d) Formulating, coordinating, and conducting the activity security education program.

d. TSCO. TSCOs are not required, but the activity head may elect to appoint a TSCO to facilitate appropriate control of Top Secret material when there is a need (e.g., accountability of Sigma 14 material as required in Volume 2 of this Manual). The TSCO maintains, for paper and other physical media (e.g., disk drives and removable computer media), a system of accountability (e.g., a registry) for activity Top Secret information and conducts inventories of Top Secret information.

(1) When collateral Top Secret information is maintained in a sensitive compartmented information facility (SCIF) or SAP secure facility, it may be handled in the same manner as SCI and SAP materials once necessary receipts have been provided to the organization supplying the materials. When collateral Top Secret material is taken out of a SCIF or SAP secure facility it shall be reentered into the registry system for accountability.

(2) Repositories, libraries, or activities that store large volumes of classified documents may limit their annual inventory to that to which access has been given in the past 12 months, and 10 percent of the remaining inventory.

(3) Accountability for Top Secret SCI, SAP, and other special types of classified information shall be in accordance with References (j) and (o), and other applicable guidance.

e. Other Security Management Roles

(1) Assistant Security Manager. In large activities and where circumstances warrant, activities may designate U.S. Government civilian or military members as assistant security manager(s) to assist the activity security manager with program implementation, maintenance, and local oversight.

(2) Security Assistants. As warranted, activities may assign U.S. Government civilian, military members, or contractor employees as security assistants to perform administrative security functions under the direction of the activity security manager without regard for job series or title or for rank, rate, or grade as long as they have the clearance required for the access needed to perform their assigned duties and tasks. (While the scope of responsibilities and job titles covered by the General Schedule (GS) 0086 Security Clerical and Assistance Series can be consistent with the duties of a security assistant as described in this paragraph, the role of security assistant as described in this paragraph does not require that civilian employees hold this job series.)

(3) Communication Security (COMSEC) Custodian. The COMSEC Custodian is the activity head's primary advisor on matters concerning the security and handling of COMSEC information and hardware and the associated records and reports and functions in accordance with NSA/CSS Policy Manual 3-16 (Reference (ak)).

(4) NATO Control Point Officer. In accordance with Reference (p), the Secretary of the Army operates the Central U.S. Registry (CUSR), the main receiving and dispatching element for NATO information in the U.S. Government. The activity NATO Control Point Officer and any designated alternate(s) ensure that NATO information is correctly controlled and accounted for and that NATO security procedures specified in Reference (q) are followed. The CUSR manages the U.S. Registry system of subregistries, communications centers, and control points to maintain accountability of NATO classified information and it conducts inspections of the associated security processes and procedures. Further information can be found at <http://www.cusr.army.mil>.

(5) SSO. An SSO is to be designated by the Senior Intelligence Official for any activity that is accredited for and authorized to receive, use, and store SCI. The activity SSO is responsible, in accordance with References (j) and (z), for the day-to-day security management, operation, implementation, use, and dissemination of SCI within the activity.

(6) SAP Security Officer. In accordance with the requirements of Reference (n), a SAP security officer is to be designated for any activity that is accredited for and authorized to receive, use, and store SAP information.

(7) Information Systems Security Officials. Information systems security officials (e.g., DAA, IAM, IA Officer) manage and oversee the DoD IT infrastructure (i.e., computer systems and networks). As computers are found everywhere within the Department of Defense, close coordination with these officials regarding implementation of security measures and procedures is imperative.

(8) CI and OPSEC. The activity's information security program must also be closely coordinated and aligned with the DoD Component's CI and OPSEC functions in order to maintain the security essential to warfighter and mission success.

7. USE OF CONTRACTORS IN SECURITY ADMINISTRATION. In accordance with DoDI 1100.22 (Reference (al)) and Office of Management and Budget Circular No. A-76 (Reference (am)), there are certain inherently governmental functions and activities that cannot be outsourced to a contractor. The DoD Components shall be careful not to outsource security functions that are inherently governmental.

a. Activity security management shall ensure that contractors who are involved in security administration and support duties are clearly identified in their capacities, roles, and functions, to ensure there is no possible confusion regarding which security personnel may exercise inherently governmental authorities and which may not.

b. Inherently governmental activities and functions include those that require either the exercise of substantial discretion in applying U.S. Government authority, or value judgments when making decisions for the U.S. Government. Inherently governmental security functions include, but are not limited to:

- (1) Approving and issuing security policies and procedures.
- (2) Making original classification decisions, or rendering classification determinations regarding classified information that is improperly or incompletely marked. (Correcting improper markings when the appropriate classification is not in question is not considered rendering a classification determination.)
- (3) Deciding to downgrade or declassify information. (Adhering to security markings on information or to guidance stated in an appropriate security classification or declassification guide is not considered a downgrading or declassification decision.)
- (4) Deciding challenges to classification and any appeals.
- (5) Making foreign disclosure decisions pursuant to Reference (u).
- (6) Making public release decisions pursuant to Reference (r).
- (7) Committing to expenditure of U.S. Government funds.
- (8) Conducting investigations of, or determining fault in, security incidents involving U.S. Government or other contractor personnel. (Contractors may conduct preliminary inquiries to determine if a security incident is a violation or an infraction.)
- (9) Giving final approval or executing documents for filing in litigation if documents assert an official position of the Department of Defense, any DoD Component, or any other Federal agency.

8. **CLASSIFICATION AUTHORITY**. Except for information subject to section 2011 et seq., of title 42, U.S.C. (also known and hereinafter referred to as “The Atomic Energy Act of 1954, as amended” (Reference (an))), Reference (d) and this Manual provide the only authority for applying security classification to information within the Department of Defense.

9. **CLASSIFICATION POLICY**. Information shall be classified only when necessary in the interests of national security and shall be declassified as soon as is consistent with the requirements of national security.

10. **RECLASSIFICATION**. After information has been declassified and released to the public under proper authority, it may be reclassified only in accordance with paragraph 17.b. of Enclosure 4.

11. ACCESS TO CLASSIFIED INFORMATION

a. Requirements for Access. Persons shall be allowed access to classified information only if they:

(1) Possess a valid and appropriate security clearance in accordance with Reference (o). Reference (o) contains detailed guidance on personnel security investigation, adjudication, and clearance.

(2) Have executed an appropriate non-disclosure agreement.

(3) Have a valid need to know the information in order to perform a lawful and authorized governmental function.

b. Nondisclosure Agreements

(1) Before being granted access to Confidential, Secret, or Top Secret information, employees shall sign SF 312, "Classified Information Nondisclosure Agreement," or other non-disclosure agreement approved by the DNI. SF 312 (or its predecessor, SF 189), or a legally enforceable facsimile retained in lieu of the original, shall be maintained for 50 years from the date of signature. Electronic signatures shall not be used to execute the SF 312.

(2) Before being granted access to SCI information, individuals adjudicated and approved for access shall sign a DNI-authorized SCI nondisclosure agreement. Consistent with the provisions of DoDD 5210.48 (Reference (ao)) and all applicable laws, that agreement shall include, as an addendum, the individual's written certification that they may be asked to undergo a polygraph examination in connection with any investigation of an unauthorized disclosure of SCI information to which they have had access.

(3) Before being granted access to SAP information, individuals adjudicated and approved for access shall additionally sign a DoD-approved program indoctrination agreement(s) for that information as required by Reference (n). Before gaining access and during a period of access to DoD SAPs, all personnel shall consent to, and be subject to, a random CI-scope polygraph examination as required by Reference (n).

c. NATO Briefing for Cleared Personnel. To facilitate potential access to NATO classified information, all DoD military and civilian personnel who are briefed on their responsibilities for protecting U.S. classified information shall be briefed simultaneously on the requirements for protecting NATO information. A written acknowledgement of the individual's receipt of the NATO briefing and responsibilities for safeguarding NATO classified information shall be maintained. As stipulated in Reference (q), access to NATO classified information shall also require a supervisor's determination of the individual's need to know and possession of the requisite security clearance. Receipt of the NATO briefing shall be verified prior to granting access to NATO classified information.

d. Access By Individuals Outside the Executive Branch. See section 6, Enclosure 2 of Volume 3 of this Manual for further guidance regarding access to classified information by individuals outside the Executive Branch.

12. PROTECTION REQUIREMENTS. Classified information and CUI shall be protected at all times. Volumes 1 through 3 of this Manual provide guidance for the protection of classified information while Volume 4 provides guidance for the protection of CUI. Additional guidance for special types of information is provided by this section.

a. Protection of Restricted Data (RD) and Formerly Restricted Data (FRD). Classified information, including Critical Nuclear Weapon Design Information (CNWDI), in the custody of the Department of Defense marked as RD or FRD in accordance with the Atomic Energy Act of 1954, as amended, shall be stored, protected, and destroyed as this Manual requires for other information of a comparable level of security classification.

(1) Consult DoDI 5210.02 (Reference (ap)) for DoD policy and procedures concerning access to and dissemination of RD, FRD, and CNWDI within the Department of Defense. Reference (ap) also provides guidance on access, distribution, handling, and accountability of Sigma information.

(2) Until DoD public key infrastructure is generally deployed on the Secret Internet Protocol Router Network (SIPRNET), the following security measures, deemed sufficient to provide the access and dissemination controls required by Reference (ap), shall be implemented when processing RD and CNWDI on SIPRNET:

(a) RD and CNWDI shall be e-mailed only after confirmation that the recipient has a final security clearance at the appropriate level, has a need to know the information, and, for CNWDI, has received the additional security briefing required by Reference (ap).

(b) All RD and CNWDI files stored on shared or personal local electronic storage devices shall be password-protected.

(c) IT systems and networks must be certified and accredited for RD, FRD, and/or CNWDI prior to transmission, processing, or storage of such data. Such certification must verify that access to RD, FRD, and CNWDI information, including through websites, is limited to authorized recipients by, at a minimum, a properly administered and protected individual identifier and password consistent with requirements of Reference (aa).

(d) System log-ons and properly configured screen savers are sufficient protection for e-mail files.

(e) In accordance with Reference (ap), Sigma 14, 15, and 20 information shall not be processed on SIPRNET.

b. Protection of SCI. SCI information shall be controlled and protected in accordance with applicable national policy, policies established by the DNI, and implementing DoD issuances. Security classification and declassification policies of this Manual apply to SCI information in the same manner as other classified information.

c. Protection of COMSEC Information. COMSEC information shall be controlled and protected in accordance with applicable national policy and DoD issuances. Security classification and declassification policies of this Manual apply to COMSEC information in the same manner as other classified information, except ONLY NSA/CSS is authorized to declassify COMSEC information.

d. Protection of SAP Information. SAPs shall be created, continued, managed, and discontinued in accordance with Reference (n) and DoDI O-5205.11 (Reference (aq)). Information covered by SAPs established in accordance with References (n) and (aq) shall be classified, declassified, controlled, and protected as this Manual, References (n) and (aq), and instructions issued by officials charged with management of those programs require. The provisions of this Manual pertaining to classification, declassification, and marking apply, without exception, to SAP information unless waivers of specific requirements are obtained in accordance with section 16 of this enclosure.

e. Protection of NATO and FGI. NATO classified information shall be safeguarded consistent with References (d) and (q). Other FGI shall be safeguarded consistent with Reference (d) and the requirements of this Manual, except as required by the Appendix to Enclosure 4 of Volume 3; treaties; or international agreements. Information that is jointly developed with a foreign partner under a cooperative program agreement will be safeguarded in accordance with the security and disclosure provisions of the cooperative arrangement.

f. Protection of Nuclear Command and Control-Extremely Sensitive Information (NC2-ESI). Certain information pertaining to the command and control of nuclear weapons is designated NC2-ESI. NC2-ESI information shall be marked, safeguarded, and distributed in accordance with CJCS Instruction 3231.01B (Reference (ar)).

13. RETENTION. Classified information and CUI shall be maintained only when it is required for effective and efficient operation of the organization or if law, treaty, international agreement, or regulation requires its retention. Such information shall be disposed in accordance with the provisions of chapter 33 of title 44, U.S.C. (Reference (as)), as implemented by DoDD 5015.2 (Reference (at)), and DoD Component implementing directives and records schedules.

14. PERMANENTLY VALUABLE RECORDS. Classified and controlled unclassified documents and material that constitute permanently valuable records of the U.S. Government shall be maintained and disposed of in accordance with Reference (at) and appropriate DoD Component directives and records schedules. Other classified and controlled unclassified material shall be destroyed as specified in this Manual. When transferring classified records for storage or archival purposes to the National Archives and Records Administration (NARA) or to

other locations, identify the boxes that contain foreign government documents as well as DoD documents containing FGI.

15. MILITARY OPERATIONS. Military commanders may modify the provisions of this Manual pertaining to accountability, dissemination, transmission, and storage of classified and controlled unclassified material and information as necessary to meet local conditions encountered during military operations. Military operations include combat and peacekeeping operations but not routine Military deployments or exercises. Classified information and CUI shall be introduced into combat areas or zones, or areas of potential hostile activity, only as necessary to accomplish the military mission.

16. WAIVERS. Unless otherwise specified herein, the DoD Components shall submit requests for waivers to the requirements of this Manual through the chain of command to the USD(I) or, for information related to foreign government (including NATO) information and security arrangements for international programs, to the USD(P). The USD(I) and USD(P) shall be responsible for promptly notifying the Director, ISOO, of approved waivers involving References (d) and (f).

a. Requests for waivers shall contain sufficient information to permit a complete and thorough analysis to be made of the impact of approval on national security. Minimally, requests must identify the specific provision(s) of this Manual for which the waiver is sought (cite volume, enclosure, and paragraph) and provide rationale and justification for the request. The request must describe the mission need and any associated risk-management considerations or provisions, including alternative or compensatory measures.

b. In the case of waivers involving classified information, the DoD Components shall maintain documents regarding approved waivers and furnish such documents to other agencies with which they share affected classified information or secure facilities, except documentation regarding approved waivers involving marking of classified information need be shared only upon request.

17. CORRECTIVE ACTIONS AND SANCTIONS

a. Procedures. Heads of the DoD Components shall establish procedures to ensure that prompt and appropriate management action is taken in cases of compromise of classified information and unauthorized disclosure of CUI, improper classification or designation of information, violation of the provisions of this Manual, and incidents that may put classified information and CUI at risk of unauthorized disclosure. Such actions shall focus on correcting or eliminating the conditions that caused or brought about the incident.

b. Sanctions

(1) DoD military and civilian personnel may be subject to criminal or administrative sanctions if they knowingly, willfully, or negligently:

(a) Disclose to unauthorized persons information properly classified in accordance with this Volume.

(b) Classify or continue the classification of information in violation of this Volume.

(c) Create or continue a SAP contrary to the requirements of Reference (n) and this Volume.

(d) Disclose CUI to unauthorized persons.

(e) Violate any other provision of this Manual.

(2) Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss, or denial of access to classified information and/or CUI, and removal of classification authority. Criminal prosecution may also be undertaken in accordance with sections 801-940 of title 10, U.S.C. (also known as “The Uniform Code of Military Justice” (UCMJ) (Reference (au))) and other applicable U.S. criminal laws.

(3) If an individual delegated OCA demonstrates reckless disregard or a pattern of error in applying the classification standards of this Volume, the appropriate official shall, as a minimum, remove the offending individual’s OCA.

c. Reporting of Incidents. Security incidents involving classified information shall be reported as required in Enclosure 6 of Volume 3 of this Manual. Incidents involving CUI shall be reported as Volume 4 requires.

ENCLOSURE 4

CLASSIFYING INFORMATION

1. CLASSIFICATION POLICY

a. Information shall be classified only to protect national security. If there is significant doubt about the need to classify information, it shall not be classified. Unnecessary or higher than necessary classification is prohibited by Reference (d). Information will be declassified as soon as it no longer qualifies for classification.

b. Classification may be applied only to information that is owned by, produced by or for, or is under the control of the U.S. Government. Information may be considered for classification only if its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security and it concerns one of the categories specified in section 1.4 of Reference (d):

- (1) Military plans, weapon systems, or operations (subsection 1.4(a));
- (2) FGI (subsection 1.4(b));
- (3) Intelligence activities (including covert action), intelligence sources or methods, or cryptology (subsection 1.4(c));
- (4) Foreign relations or foreign activities of the United States, including confidential sources (subsection 1.4(d));
- (5) Scientific, technological, or economic matters relating to the national security (subsection 1.4(e));
- (6) U.S. Government programs for safeguarding nuclear materials or facilities (subsection 1.4(f));
- (7) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security (subsection 1.4(g)); or
- (8) The development, production, or use of weapons of mass destruction (subsection 1.4(h)).

c. Information assigned a level of classification under Reference (d) or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings.

2. CLASSIFICATION PROHIBITIONS

a. Information may not be classified, continued to be maintained as classified, or fail to be declassified in order to:

(1) Conceal violations of law, inefficiency, or administrative error.

(2) Prevent embarrassment to a person, organization, or agency.

(3) Restrain competition.

(4) Prevent or delay the release of information that does not require protection in the interests of the national security.

b. Basic scientific research and its results may not be classified unless clearly related to the national security.

3. LEVELS OF CLASSIFICATION. Information identified as requiring protection against unauthorized disclosure in the interest of national security shall be classified Top Secret, Secret, or Confidential. Except as otherwise provided by statute, no other terms shall be used to identify U.S. classified information.

a. Top Secret. Top Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

b. Secret. Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.

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

4. ORIGINAL CLASSIFICATION

a. Original classification is the initial decision that an item of information could reasonably be expected to cause identifiable or describable damage to the national security if subjected to unauthorized disclosure and requires protection in the interest of national security.

b. Information may be originally classified only by the Secretary of Defense, the Secretaries of the Military Departments, and other officials to whom they delegate this authority in writing. Delegation of OCA shall be limited to the minimum number of officials required for effective operation of the Department of Defense. The authority shall be delegated to, and retained by, only those officials who have a demonstrable and continuing need to exercise it.

c. Authority to classify information at any lower level of classification is inherent in delegation of OCA.

(1) Top Secret OCA. Information may be originally classified Top Secret only by the Secretary of Defense, the Secretaries of the Military Departments, or those officials to whom the Secretary of Defense or the Secretaries of the Military Departments have delegated this authority in writing.

(2) Secret and Confidential OCA. Information may be originally classified Secret or Confidential only by the Secretary of Defense, the Secretaries of the Military Departments, and those officials to whom such authority has been delegated in writing by the Secretary of Defense, the Secretaries of the Military Departments, or the senior agency officials of the Military Departments or Department of Defense appointed in accordance with section 5.4(d) of Reference (d), provided those senior agency officials have also been delegated original Top Secret classification authority.

5. REQUESTS FOR OCA

a. Requests for OCA for officials serving in the OSD and the DoD Components, other than the Military Departments, including the Office of the Chairman of the Joint Chiefs of Staff, the Joint Staff, and the Combatant Commands, shall be submitted to the USD(I). These requests shall specify the position title for which the authority is requested, provide a brief, mission-specific justification for the request, and be submitted through established organizational channels. Heads of DoD Components, excluding the Military Departments, delegated Top Secret OCA are not authorized to delegate Secret and Confidential classification authority to subordinate officials.

b. Requests for OCA shall be approved only when:

(1) There is a demonstrable and continuing need to exercise OCA during the normal course of operations. (As a general rule, absent a security classification guide, an OCA must exercise this authority an average of twice a year to justify and retain designation as an OCA.)

(2) Such demonstrable and continuing need cannot be met through issuance of security classification guides by existing OCAs in the chain of command.

(3) Referral of decisions to existing OCAs at higher levels in the chain of command or supervision is not practical for reasons such as geographical separation.

(4) Sufficient expertise and information is available to the prospective OCA to permit effective classification decision-making.

c. OCA is designated by virtue of position. Each OCA delegation shall be in writing and the authority shall not be redelegated except as provided in paragraph 4.c. of this enclosure. Each

delegation shall identify the official to whom authority is delegated by position title. The Director of Security, OUSD(I), shall be notified in writing of all OCA delegations.

(1) Only senior positions (typically general and/or flag officer or Senior Executive Service or equivalent level) assigned a unique mission with responsibility in one of the subject areas cited in paragraph 1.b. of this enclosure may be designated an OCA.

(2) Deputies, vice commanders, chiefs of staff, and similar immediate subordinates of an OCA are empowered to exercise the OCA when they have been officially designated to assume the duty position of the OCA in an “acting” capacity during the OCA’s absence and have certified in writing that they have received the OCA training required by Enclosure 5 of Volume 3 of this Manual.

d. Before exercise of the authority and annually thereafter, persons in positions with delegated OCA must certify in writing that they have received training in the fundamentals of proper security classification and declassification, the limitations of their authority, the sanctions that may be imposed, and OCA duties and responsibilities, as required by Enclosure 5 of Volume 3 of this Manual.

e. Activity security managers must ensure that OCA delegation letters and OCA training certifications are maintained and can be retrieved by the office assigned that responsibility when requested by appropriate authorities.

6. ORIGINAL CLASSIFICATION PROCESS. All DoD OCAs are responsible to the Secretary of Defense for their classification decisions. In making a decision to originally classify information, they shall:

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

b. Determine the information falls within one or more of the categories of information listed in paragraph 1.b. of this enclosure.

c. Determine the information has not already been classified by another OCA.

d. Determine that classification guidance is not already available in the form of security classification guides, plans, or other memorandums. Within the Department of Defense, the majority of existing classification guidance is indexed and promulgated via the DTIC, available at www.dtic.mil.

e. Determine that there is a reasonable possibility that the information can be provided protection from unauthorized disclosure. OCAs shall balance the cost to protect the information against the risks associated with its disclosure. The advantages must outweigh the disadvantages of classification.

f. Determine and assign the appropriate level of classification (i.e., Top Secret, Secret, or Confidential) to be applied to the information, based on reasoned judgment as to the degree of damage, which the OCA can describe, that could be caused by unauthorized disclosure. If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

(1) Determine the probable operational, technological, and resource impact of classification.

(2) If decisions must be rendered verbally due to exigencies of an ongoing operation or other emergency, issue written confirmation within 7 calendar days of the decision and provide the required declassification and marking instructions.

(3) Be prepared to present, as required, depositions and expert testimony in courts of law concerning classification of national security information and to justify their original decisions.

(4) Be prepared to produce a written description of the damage, as necessary, for a classification challenge, a security classification review, a damage assessment, a request for mandatory review for declassification, a request for release under section 552 of title 5, U.S.C. (also known and hereinafter referred to as "The Freedom of Information Act" (FOIA) (Reference (av))), when pertinent to judicial proceedings, or as other statute or regulation may require.

g. Determine the appropriate duration of classification to be applied to the information. Section 13 of this enclosure discusses the specific options available in making this decision.

h. Document the classification decision and clearly and concisely communicate it in writing to persons who shall possess the information by issuing classification guidance or by ensuring documents containing the information are properly marked to reflect the decision. Classification guidance may be communicated by issuance of a security classification or declassification guide or in the form of a memorandum, plan, order, or letter. If issued by other than a classification or declassification guide, the guidance should be incorporated in a guide in a timely fashion. Enclosure 6 of this Volume discusses classification guides; Volume 2 of this Manual provides marking guidance.

7. CHANGING THE LEVEL OF CLASSIFICATION. OCAs may change the level of classification of information under their jurisdiction, provided the information continues to meet the standards for classification identified in this enclosure. Documents shall be re-marked with the new classification level, the date of the action, and the authority for the change. Changing the classification level may also require changing portion markings for information contained within the document. Additionally, the OCA shall update appropriate security classification guides and immediately notify all known holders of the information of the changes. Sections 18 and 19 of Enclosure 5 of this Volume provide additional guidance on downgrading and upgrading classified information.

8. SECURITY CLASSIFICATION GUIDANCE

a. The responsible OCA shall issue security classification guidance for each system, plan, program, project, or mission involving classified information. Classification guidance may be in the form of a memorandum, plan, order, or letter, or issuance of a security classification or declassification guide.

b. OCAs shall develop, as appropriate, automatic and systematic declassification guidance for use in review of records that are of permanent historical value and 25 years old or older. This guidance shall be published in the appropriate classification or declassification guide.

c. Exemptions from automatic declassification approved pursuant to section 13 of Enclosure 5 of this Volume may be incorporated into classification guides provided the ISCAP is notified of the intent to take such action in advance and the information remains in active use. See paragraph 13.c. of Enclosure 5 of this Volume for the notification process.

d. Where classification guidance is issued in the form of a security classification guide, the OCA shall ensure the guide is reviewed and updated as specified in Enclosure 6 of this Volume.

e. As a general rule, classification authority must be exercised an average of twice a year to qualify for retention of the OCA designation if an OCA does not issue and maintain a security classification guide.

9. TENTATIVE CLASSIFICATION. Individuals who submit information to OCAs for original classification decisions shall provide the OCA the information required by paragraphs 6.a. through 6.f. of this enclosure, and may, as necessary, tentatively classify information or documents as working papers, pending approval by the OCA. Final classification decisions must be made as soon as possible, but not later than 180 days from the initial drafting date of the document. Prior to the OCA's classification decision, such information shall be safeguarded as required for the specified level of classification and it shall not be used as a source for derivative classification.

10. DERIVATIVE CLASSIFICATION

a. When incorporating, paraphrasing, restating, or generating classified information in a new form or document (i.e., derivatively classifying information), it must be identified as classified information by marking or similar means. Derivative classification includes classification of information based on classification guidance in a security classification guide or other source material, but does not include photocopying or otherwise mechanically or electronically reproducing classified material.

b. Within the Department of Defense all cleared personnel, who generate or create material that is to be derivatively classified, shall ensure that the derivative classification is accomplished in accordance with this enclosure. No specific, individual delegation of authority is required.

DoD officials who sign or approve derivatively classified documents have principal responsibility for the quality of the derivative classification.

c. All persons performing derivative classification shall receive training, as specified in Enclosure 5 of Volume 3 of this Manual, on proper procedures for making classification determinations and properly marking derivatively classified documents.

11. RESPONSIBILITIES OF DERIVATIVE CLASSIFIERS. Derivative classifiers shall:

a. Observe and respect the classification determinations made by OCAs. If derivative classifiers believe information to be improperly classified, they shall take the actions required by section 22 of this enclosure.

b. Identify themselves and the classified information by marking it in accordance with Volume 2 of this Manual.

c. Use only authorized sources for classification guidance (e.g., security classification guides, memorandums, DoD publications, and other forms of classification guidance issued by the OCA) and markings on source documents from which the information is extracted for guidance on classification of the information in question. The use of memory alone or “general rules” about the classification of broad classes of information is prohibited.

d. Use caution when paraphrasing or restating information extracted from a classified source document. Paraphrasing or restating information may change the need for or level of classification.

e. Take appropriate and reasonable steps, including consulting a security classification guide or requesting assistance from the appropriate OCA, to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification. In cases of apparent conflict between a security classification guide and a classified source document regarding a discrete item of information, the instructions in the security classification guide shall take precedence. Where required markings are missing or omitted from source documents, consult the OCA, appropriate security classification guide, or other classification guidance for application of the omitted markings.

12. PROCEDURES FOR DERIVATIVE CLASSIFICATION

a. Derivative classifiers shall carefully analyze the material they are classifying to determine what information it contains or reveals and shall evaluate that information against the instructions provided by the classification guidance or the markings on source documents.

b. Drafters of derivatively classified documents shall portion-mark their drafts and keep records of the sources they use, to facilitate derivative classification of the finished product.

c. When material is derivatively classified based on “multiple sources” (i.e., more than one security classification guide, classified source document, or combination thereof), the derivative classifier shall compile a list of the sources used. This list shall be included in or attached to the document.

d. Duration of classification for derivatively classified documents shall be determined in accordance with section 13 of this enclosure and applied in accordance with Volume 2 of this Manual. The instructions shall not be automatically copied from source documents without consideration of adjustments that may be required (e.g., due to use of multiple sources, changes in policy, changes in classification guidance).

e. If extracting information from a document or section of a document classified by compilation, the derivative classifier shall consult the explanation on the source document to determine the appropriate classification. If that does not provide sufficient guidance, the derivative classifier shall contact the originator of the source document for assistance.

f. Infrequently, different sources of classification guidance may specify different classification for the same information. When such inconsistencies are encountered, the derivative classifier must contact the applicable OCA(s) for resolution of the inconsistency. Pending determination, the document or material containing the information shall be protected at the highest level of classification specified by the sources.

13. DURATION OF CLASSIFICATION. Every time a classified document is created, a determination must be made regarding how long the information is to be protected (i.e., when the information will lose its sensitivity and no longer merit or qualify for classification). This is an essential part of the classification process.

a. Originally Classified Information. At the time an item of information is classified, the OCA shall establish a specific date or event for declassification, based on the duration of the national security sensitivity of the information. The OCA shall use one of the following duration options, selecting, whenever possible, the one that will result in the shortest duration of classification.

(1) A date or independently verifiable event less than 10 years from the date of the document;

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

(3) A date or independently verifiable event greater than 10 and less than 25 years from the date of the document;

(4) A date 25 years from the date of the document;

(5) “50X1-HUM,” designating a duration of up to 75 years, when classifying information that could clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source;

(6) “50X2-WMD,” designating a duration of up to 75 years, when classifying information that could clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction; or

(7) “25X” with date or event, designating a duration of up to 50 years when classifying information that clearly falls within an exemption from automatic declassification at 25 years that has previously been approved by the ISCAP.

b. Derivatively Classified Information. For derivatively classified information, the most restrictive declassification instruction (i.e., the one that specifies the longest duration of classification) must be carried forward from the source document(s), security classification guide(s) or other classification guidance provided by the OCA. Specific guidance on determining the most restrictive instruction is provided in Enclosure 3 of Volume 2.

c. Extending the Duration of Classification. Information is declassified on the date or event specified by the OCA unless the OCA takes action to extend the duration of classification.

(1) If the date or event for declassification specified by the OCA has not passed, an OCA may extend the duration of classification for information under their jurisdiction, provided the information continues to meet the standards for classification. The period of classification shall not exceed 25 years from the date of the document’s origin. When extending the duration of classification, the OCA must immediately notify all known holders of the information of the extension.

(2) If the date or event specified by the OCA has passed, the information may be reclassified only in accordance with sections 17 and 18 of this enclosure.

14. FORMAT FOR DISSEMINATION. Whenever practicable, OCAs and derivative classifiers shall use a classified attachment, addendum, annex, enclosure, or similar section if the classified information constitutes only a small portion of an otherwise unclassified document. Alternately, a separate product that would allow dissemination at the lowest level of classification possible or in unclassified form may be prepared.

15. COMPILATIONS

a. Compilations of information that are individually unclassified (or classified at a lower level) may be classified (or classified at a higher level) only if the compiled information reveals an additional association or relationship that:

(1) Qualifies for classification pursuant to paragraph 1.b. of this enclosure, and

(2) Is not otherwise revealed by the individual elements of information.

b. OCAs shall use the same decision process as for other information when determining whether compilations of individual items require classification.

(1) Classification as a result of compilation must meet the same criteria in terms of justification as other original classification actions (see section 6 of this enclosure).

(2) The information must be located where one could realistically assume that the elements of information could be associated to derive classified meaning. Note that user queries of data in electronic formats (e.g., databases, spreadsheets) lead to new aggregations, and posting of information on the Internet makes the use of data mining and other data correlation tools easy and widespread. OCAs should consider the possibility that such tools and methods will be used to compile information and should, when appropriate, identify classified compilations when issuing classification guidance.

c. Classification as a result of compilation requires an original classification decision by an authorized OCA or classification guidance issued by an OCA (e.g., a security classification guide).

(1) The final decision regarding classification of compiled data resides with the OCA who has purview over the program that creates or generates the compilation. However, the program manager or other official responsible for the database, application, or program that creates or generates the compilation is responsible for facilitating, as necessary, a security classification review with other appropriate OCAs for the constituent items of information. Assistance from the servicing security, OPSEC, and CI offices is recommended, but the responsibility for the review resides with the program manager or other responsible official. Where the individual OCAs are unable to agree on the classification of the aggregated data, the decision may be raised to an official higher in the chain of command who is authorized OCA and has program or supervisory authority over the data.

(2) A classification by compilation decision must honor (i.e., cannot overrule or change) previous decisions by an OCA regarding the classification of individual elements or of the compilation. As part of the classification decision process, officials should determine whether the compilation has previously been classified by another OCA.

(3) OCAs must avoid using classification as a means to protect information merely because the compiled data represents a significant amount of information available in one place (e.g., in an authoritative data source), unless damage to the national security can be articulated as required by section 6 of this enclosure. When information qualifies for classification as a result of compilation, it is because the whole is greater than the sum of the parts (i.e., something new is revealed by putting all of the pieces together that is not revealed by the individual parts). Classification of compilations presents its own set of issues, not the least of which is determining how to handle and share individual pieces of information without creating the possibility for inadvertent compilation of the whole.

(4) The classification of each element of a classified compilation must be clearly identified by portion marking or explanation, as appropriate, so that when separated the classification of each individual element can be determined. OCAs are reminded of the requirement to clearly describe the basis for the classification as a result of compilation when originally classifying the compilation (see marking requirements in section 12, Enclosure 3 of Volume 2 of this Manual). If the classification of an individual element cannot be determined, the information shall be protected at the level of classification of the compilation and the OCA contacted for specific guidance.

d. When specific combinations of unclassified data elements are known to be classified (or specific combinations of data elements classified at a lower level qualify for classification at a higher level), the OCA must identify these combinations and document them in security classification guides. The program manager or other responsible official and the OCA(s) should review the elements of information used by their program(s) as early in the program as possible to determine if there are obvious or likely compilations that reveal relationships or associations that require classification.

e. Where specific combinations of unclassified data elements are known to be classified, CONSISTENTLY withholding specified data elements from public Internet posting and, to the extent possible consistent with statute and other regulations, public release can mitigate the ability of others to create the classified compilation. Thus, OCAs should consider including in security classification guides, where appropriate, prohibitions on posting one or more of the specific data elements that are known to make up a classified compilation of unclassified data elements to publicly accessible Internet sites.

16. CLASSIFICATION OF ACQUISITION INFORMATION. Classifying information involved in the DoD acquisition process shall conform to the requirements of DoDD 5000.01 (Reference (aw)) and DoDI 5000.02 (Reference (ax)), as well as this enclosure. Security classification guides should be updated to include classified critical program information identified as part of the program protection planning process required by DoDI 5200.39 (Reference (ay)).

17. CLASSIFICATION OF INFORMATION RELEASED TO THE PUBLIC

a. Classified Information Released Without Proper Authority

(1) Classified information that has been released to the public without proper authority (e.g., media leak, data spill) may remain classified or may be declassified upon such determination by the appropriate OCA. Enclosure 6 of Volume 3 of this Manual identifies issues to be considered when making the decision. When the determination is made that the information will remain classified, the appropriate OCA will notify known authorized holders accordingly and provide the following marking guidance to be used in the event the information is not marked:

- (a) Overall level of classification.
- (b) Portion markings.
- (c) Identity, by name or personal identifier and position, of the OCA.
- (d) Declassification instructions.
- (e) Concise reason for classification.
- (f) Date the action was taken.

(2) Holders of the information shall take administrative action, as needed, to apply markings and controls. DoD personnel shall not publicly acknowledge the release of classified information and must be careful not to make any statement or comment that confirms the accuracy of or verifies the information requiring protection.

b. Reclassification of Information Declassified and Released to the Public Under Proper Authority

(1) Information that has been declassified and released to the public under proper authority may be reclassified only when:

(a) The information may be reasonably recoverable without bringing undue attention to the information, which means that:

1. Most individual recipients or holders are known and can be contacted and all forms of the information to be reclassified can be retrieved from them.

2. If the information has been made available to the public via means such as U.S. Government archives or reading rooms, it can be or has been withdrawn from public access without significant media or public attention or notice.

(b) The Secretary of Defense approves the reclassification based on a document-by-document determination and recommendation by the Head of the originating DoD Component, other than the Secretary of a Military Department, that reclassification of the information is required to prevent significant and demonstrable damage to the national security. Declassification and release of information under proper authority means the DoD Component with jurisdiction over the information authorized declassification and release of the information. The Secretaries of a Military Department shall approve the reclassification of information under their jurisdiction on the same basis and shall notify the USD(I) of the action. The Military Departments shall provide implementing guidance to their subordinate activities for submitting such requests.

(2) DoD Component Heads other than the Secretaries of the Military Departments shall submit recommendations for reclassification of information under their jurisdiction to the

Secretary of Defense through the USD(I). Recommendations for reclassification must include, on a document-by-document basis:

- (a) A description of the information.
- (b) All information necessary for the original classification decision in accordance with section 6 of this enclosure, including classification level of the information and declassification instructions to be applied.
- (c) When and how it was released to the public.
- (d) An explanation as to why it should be reclassified. Include the applicable reason in accordance with Reference (d) and describe what damage could occur to national security. Also describe what damage may have already occurred as a result of the release.
- (e) The number of recipients and/or holders and how they will be notified of the reclassification.
- (f) How the information will be recovered.
- (g) Whether the information is in the custody of NARA and whether the Archivist of the United States must be notified of the reclassification as specified in subparagraph 17.b.(4) of this section.

(3) Once a reclassification action has occurred, it must be reported to all recipients and holders, to the Assistant to the President for National Security Affairs (herein after referred to as “the National Security Advisor”) and to ISOO within 30 days. The notification to ISOO must include how the “reasonably recoverable” decision was made, including the number of recipients or holders, how the information was recovered, and how the recipients and holders were notified. The Secretaries of the Military Departments shall notify the National Security Advisor and ISOO directly and provide an information copy to USD(I). The Secretary of Defense, after making reclassification decisions, will notify the National Security Advisor and ISOO of such decisions.

(4) For documents in the physical and legal custody of NARA that have been available for public use, reclassification must also be reported to the Archivist of the United States, who shall suspend public access pending approval of the reclassification action by the Director, ISOO. The Secretaries of the Military Departments shall notify the Archivist directly and provide an information copy to USD(I). The Secretary of Defense will notify the Archivist as required for decisions involving other DoD Components. Disapproval of the reclassification action by the Director, ISOO, may be appealed to the President through the National Security Advisor. Public access shall remain suspended pending decision on the appeal.

(a) OCAs shall notify the Secretary of Defense of the need to appeal ISOO decisions through their DoD Component Head and the USD(I).

(b) Notifications shall clearly articulate the compelling national security reasons for

reclassifying the information and shall counter the ISOO rationale for disapproving the reclassification.

(5) Once a final decision is rendered, OCAs shall update their security classification guidance accordingly. The reclassified information must be marked and safeguarded in accordance with the requirements of Volumes 2 and 3 of this Manual.

(6) Any cleared recipients or holders of reclassified information shall be notified and appropriately briefed about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure. The recipients or holder who do not have security clearances shall, to the extent practicable, be appropriately briefed about the reclassification of the information to which they have had access and their obligation not to disclose the information, and shall be asked to sign an acknowledgement of the briefing and to return all copies of the information in their possession.

c. Information Declassified and Released to the Public Without Proper Authority. Information that was declassified without proper authority remains classified. See paragraph 17.a. of this enclosure and paragraph 1.c. of Enclosure 5 of this Volume.

18. CLASSIFICATION OR RECLASSIFICATION FOLLOWING RECEIPT OF A REQUEST FOR INFORMATION. Information that has not previously been released to the public under proper authority may be classified or reclassified after receiving a request for it under FOIA; section 2204(c)(1) of Reference (as) (also known as “The Presidential Records Act of 1978”); section 552a of Reference (av) (also known and hereinafter referred to as “The Privacy Act of 1974, as amended”); or the mandatory review provisions of section 3.5 of Reference (d), only if it is done on a document-by-document basis with the personal participation or under the direction of the USD(I), the Secretary or Under Secretary of a Military Department, or the senior agency official appointed within a Military Department in accordance with section 5.4(d) of Reference (d). OCAs shall submit requests to the USD(I) through the Head of the DoD Component.

a. The provisions of this section apply to information that has been declassified in accordance with the date or event specified by the OCA as well as to information not previously classified.

b. Classification requests shall provide all information necessary for the original classification process as specified by section 6 of this enclosure.

c. The Secretaries of the Military Departments shall notify the USD(I) of classification decisions made in accordance with the provisions of this section.

d. Once a decision is rendered, OCAs shall update their security classification guidance as needed.

19. CLASSIFYING NON-GOVERNMENT RESEARCH AND DEVELOPMENT INFORMATION

a. Information that is a product of contractor or individual independent research and development (IR&D) or bid and proposal (B&P) efforts, as defined by DoDD 3204.1 (Reference (az)), conducted without prior or current access to classified information associated with the specific information in question may not be classified unless:

(1) The U.S. Government first acquires a proprietary interest in the information; or,

(2) The contractor or individual conducting the IR&D or B&P requests that the U.S. Government contracting activity place the information under the control of the security classification system without relinquishing ownership of the information.

b. The contractor or individual conducting such an IR&D or B&P effort and believing that the information generated may require protection in the interest of national security shall safeguard the information and submit it to an appropriate U.S. Government activity for a classification determination.

(1) The U.S. Government activity receiving the request shall issue security classification guidance, as appropriate, if the information is to be classified. If the information is not under the activity's classification authority, the activity shall refer the matter to the appropriate classification authority and inform the individual or contractor of the referral. The information shall be safeguarded until the matter is resolved.

(2) The U.S. Government activity authorizing classification for the information shall verify whether the contractor or individual is cleared and has been authorized to store classified information. If not, the U.S. Government activity authorizing classification shall advise whether clearance action should be initiated.

(3) If the contractor or individual refuses to be processed for the appropriate security clearance and the U.S. Government does not acquire a proprietary interest in the information, the information may not be classified.

(4) If the information is not classified, consideration may be given to the need for other controls applicable to unclassified information (e.g., export controls). (See Volume 4 of this Manual for guidance on CUI.)

20. THE PATENT SECRECY ACT OF 1952. Sections 181 through 188 of title 35, U.S.C. (also known and hereinafter referred to as "The Patent Secrecy Act of 1952" (Reference (ba))) provides that the Secretary of Defense, among others, may determine that disclosure of an invention by granting of a patent would be detrimental to the national security. The Department of Defense shall handle a patent application on which a secrecy order has been imposed as follows:

a. If the patent application contains information that warrants classification, it shall be assigned a classification and be marked and safeguarded accordingly.

b. If the patent application does not contain information that warrants classification:

(1) Place a cover sheet (or cover letter for transmittal) on the application with a statement substantially like that shown in Figure 1, changing the classification as appropriate.

Figure 1. Patent Secrecy Act Statement

The attached material contains information on which secrecy orders have been issued by the U.S. Patent Office after determination that disclosure would be detrimental to national security (Patent Secrecy Act of 1952, 35 U.S.C. 181-188). Its transmission or revelation in any manner to an unauthorized person is prohibited by law. Handle as though classified CONFIDENTIAL (or other classification as appropriate).

(2) Withhold the information from public release.

(3) Control its dissemination within the Department of Defense.

(4) Instruct the applicant not to disclose the information to any unauthorized person.

(5) Safeguard the patent application, or other document incorporating the protected information, in the manner prescribed for equivalent classified material.

c. If filing of a patent application with a foreign government is approved in accordance with provisions of the Patent Secrecy Act of 1952 and agreements on interchange of patent information for defense purposes, mark the copies of the patent application prepared for foreign registration (but only those copies) at the bottom of each page with the statement shown in Figure 2.

Figure 2. Patent Secrecy Act Foreign Registration Statement

Withheld under the Patent Secrecy Act of 1952 (35 U.S.C. 181-188)
Handle as [insert CONFIDENTIAL
or such other level as has been determined appropriate].

21. REQUESTS FOR CLASSIFICATION DETERMINATION. Within 30 days of receipt OCAs shall provide a classification determination to requests for same from individuals who are not OCAs, but who believe they have originated information requiring classification. If the information is not under the OCA's classification authority, the request shall be referred to the

appropriate OCA and the requestor shall be informed of the referral. Pending a classification determination the information shall be protected consistent with the requirements of this Manual.

22. CHALLENGES TO CLASSIFICATION

a. Principles. If holders of information have substantial reason to believe that the information is improperly or unnecessarily classified, they shall communicate that belief to their security manager or the OCA to bring about any necessary correction. This may be done informally or by submitting a formal challenge to the classification in accordance with References (d) and (f).

(1) Informal questioning of classification is encouraged before resorting to formal challenge. If the information holder has reason to believe the classification applied to information is inappropriate, he or she should contact the classifier of the source document or material to resolve the issue.

(2) The Heads of the DoD Components shall ensure that no retribution is taken against any individual for questioning a classification or making a formal challenge to a classification.

(3) Formal challenges to classification made pursuant to this section shall include sufficient description of the information being challenged to permit identification of the information and its classifier with reasonable effort. Challenges to classification made by DoD personnel shall also include the reason why the challenger believes that the information is improperly or unnecessarily classified. The challenge shall be unclassified, if possible.

(4) Information that is the subject of a classification challenge shall remain classified and continue to be safeguarded unless and until a decision is made to declassify it.

(5) The provisions of this section do not apply to information required to be submitted for prepublication review or other administrative process pursuant to an approved NDA.

b. Procedures. The Heads of the DoD Components shall establish procedures for handling challenges to classification received from within and from outside their Components in accordance with Reference (f). The DoD Components shall:

(1) Establish a system for processing, tracking, and recording formal challenges to classification, including administrative appeals of classification decisions, and ensure that DoD Component personnel are made aware of the established procedures for classification challenges.

(2) Provide an opportunity for review of the information by an impartial official or panel.

(3) Except as provided in subparagraphs 22.b.(4) and (5) of this section, provide an initial written response to each challenge within 60 days. If not responding fully to the challenge within 60 days, the DoD Component shall acknowledge the challenge and provide an expected date of response. This acknowledgment shall include a statement that, if no response is received

within 120 days, the challenger has the right to forward the challenge to the ISCAP for decision. The challenger may also forward the challenge to the ISCAP if the Component has not responded to an appeal within 90 days of receipt of the appeal. DoD Component responses to those challenges it denies shall include the challenger's right to appeal to the ISCAP.

(4) Not process the challenge if it concerns information that has been the subject of a challenge within the preceding 2 years or is the subject of pending litigation. The DoD Component shall inform the challenger of the situation and appropriate appellate procedures.

(5) Refer challenges involving RD to the Department of the Energy and FRD to the Deputy Assistant Secretary of Defense, Nuclear Matters (DASD(NM)) and notify the challenger accordingly. Do not include a statement about forwarding the challenge to the ISCAP in the notification letter, as these categories of information are not within the purview of the ISCAP.

(6) In case a classification challenge involves documents that contain RD and/or FRD as well as information classified under Reference (d), delete (redact) the RD and FRD portions of the documents before the document is forwarded to the ISCAP for review.

ENCLOSURE 5

DECLASSIFICATION AND CHANGES IN CLASSIFICATION

1. DECLASSIFICATION POLICY

a. Per Reference (d), information shall be declassified as soon as it no longer meets the standards for classification. In some exceptional cases, the need to protect information still meeting these standards may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. Pursuant to DoD policy in Reference (b), information shall remain classified only as long as:

- (1) It is in the best interest of national security to keep it protected.
- (2) Continued classification is in accordance with the requirements of Reference (d).

b. If DoD officials have reason to believe that the public interest in disclosure of information outweighs the need for continued classification, they shall refer the matter to the appropriate senior agency official appointed in accordance with section 5.4(d) of Reference (d), who shall consult with the OCA. The senior agency official shall determine whether to declassify the information.

c. Classified information that has been declassified without proper authority remains classified until declassified by an OCA with jurisdiction over the information.

- (1) Administrative action shall be taken to restore markings and controls, as appropriate.
- (2) If the information is in records in the physical and legal custody of NARA and has been made available to the public:
 - (a) The OCA shall, as part of determining if restoration of markings and controls is appropriate, consider whether removing the information from public access will significantly mitigate harm to the national security or otherwise draw undue attention to the information.

(b) DoD or Military Department senior agency official shall provide written notification to the Archivist of the United States, which shall include a description of the record(s), the elements of information that are classified, the duration of classification, and the specific authority for continued classification. OCAs in DoD Components other than the Military Departments shall submit notifications to USD(I), through their chain of command, for submission to the Archivist.

(c) The issue shall be referred to the Director, ISOO if the information is more than 25 years old and the Archivist does not agree with the OCA's determination that the information remains classified. The information shall be withdrawn from public access pending resolution.

d. Classified information shall be marked as declassified, as specified by Enclosure 3 of Volume 2 of this Manual, before it is handled as unclassified. Holders of classified information marked with a date or event on the “declassify on” line shall, when the date or event has passed, confirm that the OCA(s) of 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. Once declassification is confirmed, such information may be made publicly available only as provided in paragraph 1.e of this section.

e. Declassification does not authorize release of the information to the public. **DECLASSIFIED INFORMATION SHALL NOT BE RELEASED TO THE PUBLIC UNTIL A PUBLIC RELEASE REVIEW AS REQUIRED BY REFERENCES (R) AND (S) HAS BEEN CONDUCTED** to determine if there are reasons for withholding some or all of the information. Declassified information may be released to the public unless withholding is appropriate in accordance with other applicable law (for example, FOIA or the Privacy Act of 1974, as amended) or DoD issuance (for example, Reference (r) and DoDD 5230.25 (Reference (bb))). Regardless of the date specified for declassification, declassified information shall not be approved for public release without referral to the OCA of the information, except records accessioned by NARA that were reviewed for automatic declassification in accordance with section 3.3 of Reference (d) will be reviewed by NARA for public release.

f. Personnel leaving DoD employment or service may not direct that information be declassified in order to remove it from DoD control.

g. OCAs affected by ISCAP deliberations shall be notified of the final decision and shall consider the need to change classification and declassification guides to reflect the specific ISCAP decision.

2. PROCESSES FOR DECLASSIFICATION. Reference (d) establishes four separate and parallel processes for declassifying information:

a. A process requiring the original classifier to decide at the time information is classified when it may be declassified.

b. A process that shall cause information of permanent historical value to be automatically declassified no later than 31 December of the year that is 25 years from the date of its origin unless specific action is taken to keep it classified.

c. A process for reviewing information for possible declassification upon request (mandatory declassification review).

d. A process for systematic review of information for possible declassification.

3. AUTHORITY TO DECLASSIFY

a. Information may be declassified or downgraded by the cognizant OCA, by supervisory officials of the OCA if the supervisory official has OCA, or by those officials who have been delegated declassification authority in accordance with paragraph 3.b. of this enclosure. The authority to declassify information extends only to information for which the specific official has classification, program, or functional responsibility.

b. DoD Component Heads with OCA may designate officials within their organizations to exercise declassification authority (e.g., make declassification decisions, issue declassification guidance) over specific types or categories of information for which they are responsible. Delegations of declassification authority shall be reported concurrently to the Director of Security, OUSD(I). Other OCAs may designate members of their staffs to exercise declassification authority over information under their jurisdiction. Declassification authorities, other than original classifiers, shall receive training as specified in section 6 of Enclosure 5, Volume 3 of this Manual upon initial designation and every 2 years thereafter.

c. Pursuant to section 7 of this enclosure, only NSA/CSS is authorized to downgrade or declassify cryptologic information.

d. If the activity originating the classified information no longer exists, the activity that inherited the functions of the originating activity shall determine what constitutes appropriate declassification action. If the functions of the originating activity were dispersed to more than one activity, the inheriting activity(ies) cannot be determined, or the functions have ceased to exist, the senior agency official of the DoD Component of the originating activity shall determine the declassification action to be taken.

e. Information originated by another agency or DoD Component shall be referred to the originator for downgrading or declassification determinations.

4. DECLASSIFICATION GUIDANCE. Persons with declassification authority shall develop and issue declassification guidance to facilitate effective review and declassification of information classified under both current and previous classified national security information Executive orders. The guidance may be in the form of declassification guides, sections of security classification guides, memorandums, etc. Exemptions authorized in accordance with section 13 of this enclosure should be cited in declassification guidance.

5. DECLASSIFICATION OF INFORMATION

a. Holders of classified information marked with a date or event on the “declassify on” line, shall, prior to downgrading or declassifying the information, confirm that the OCA(s) for the information has not extended the classification period.

b. Holders of classified information may confirm the classification period (i.e., date or event for declassification) by reference to the applicable security classification or declassification

guide or other appropriate guidance issued by the OCA(s), or by consultation with the OCA(s). Classified information shall continue to be safeguarded as required for the indicated classification level until the holder has confirmed that the OCA(s) has not extended the classification period.

c. If the holder of a document has reason to believe it should not be declassified as specified, the originator shall be notified through appropriate administrative channels. The document or material shall continue to be protected at the originally assigned classification until the issue is resolved.

d. Declassification markings are used to clearly convey the declassified status of the information and who authorized the declassification. All declassified information in agency records not held by NARA shall have the declassification markings required by Enclosure 3 of Volume 2 of this Manual applied.

6. CANCELING OR CHANGING CLASSIFICATION MARKINGS. Declassification authority is not required for simply canceling or changing classification markings in accordance with guidance from an OCA or declassification authority. Sections 18 and 19 of this enclosure provide guidance on downgrading and upgrading classified information.

7. SPECIAL PROCEDURES FOR CRYPTOLOGIC INFORMATION. Only NSA/CSS may declassify cryptologic information. Therefore, such information uncovered in systematic or mandatory review of U.S. Government records for declassification, including such information incorporated into other documents, must be referred to the NSA/CSS for declassification determination.

a. Recognition of cryptologic information is not always easy since it may concern or reveal the processes, techniques, operations, and scope of signals intelligence, which consists of communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, or it may concern IA, which includes COMSEC, including the communications portion of cover and deception plans. Much cryptologic information is also considered FGI.

b. NSA/CSS has established special procedures for mandatory review for declassification of classified cryptologic information. For questions regarding cryptographic equities or for referrals for declassification determination, contact:

Director, National Security Agency/
Chief, Central Security Service
ATTN: Declassification Services (DJP5)
Fort George G. Meade, MD 20755-6248

8. PERMANENTLY VALUABLE RECORDS

a. Classified information in records that are scheduled for retention by NARA as permanently valuable records when that information is less than 20 years old shall be subject to the automatic declassification provisions of section 12 of this enclosure when the information is 25 years old.

b. Classified information in records that are scheduled for retention by NARA as permanently valuable records when that information is already more than 20 years old shall be subject to the automatic declassification provisions of section 12 of this enclosure 5 years from the date the records are scheduled.

9. RECORDS DETERMINED NOT TO HAVE PERMANENT HISTORICAL VALUE.

Classified records determined not to be permanently valuable and not scheduled retention by NARA are subject to the automatic declassification provisions of this issuance. The disposition (destruction) date of those records in the DoD Component's Records Control Schedule or General Records Schedule approved by NARA shall be used as the declassification date, although the duration of classification may be extended if a record has been retained for business reasons beyond its scheduled destruction date. If the disposition date extends beyond 25 years, an exemption request must be submitted to and approved by the ISCAP in accordance with the procedure in section 13 of this enclosure.

10. EXTENDING CLASSIFICATION BEYOND 25 YEARS FOR UNSCHEDULED

RECORDS. For unscheduled classified records (both permanent and temporary), the duration of classification beyond 25 years shall be determined when the records are scheduled (i.e., when NARA has approved a records control schedule that can be used to determine their final disposition). Permanently valuable records must be scheduled before they are 25 years old in order to request ISCAP approval to extend classification beyond 25 years when applicable. Contact the DoD Component Records Manager for further guidance on scheduling records.

11. CLASSIFIED INFORMATION IN THE CUSTODY OF CONTRACTORS, LICENSEES, GRANTEEES, OR OTHER AUTHORIZED PRIVATE ORGANIZATIONS OR INDIVIDUALS.

Pursuant to the provisions of Reference (x), DoD Components must provide security classification and declassification guidance to contractors, licensees, grantees, or other authorized private organizations or individuals who possess DoD classified information. DoD Components must also determine if classified records are held by such entities, and, if so, whether they are permanent records of historical value and thus subject to automatic declassification. Until such a determination has been made by an appropriate official, the classified information contained in such records shall not be subject to automatic declassification and shall be safeguarded in accordance with the most recent security classification or declassification guidance provided by the DoD Component.

12. AUTOMATIC DECLASSIFICATION. Reference (d) establishes a system for declassification of information in permanently valuable historical records. DoD Component

declassification activities shall conduct reviews of records eligible for automatic declassification in accordance with the procedures specified in this enclosure and Reference (f) and by the NDC and/or the JRC.

a. Deadline. All permanently valuable records shall be reviewed for declassification by December 31 of the year in which they become 25 years old. Unless the document warrants continued classification in accordance with an authorized exclusion (see paragraph 12.e of this section) or an ISCAP-approved exemption (see section 13 of this enclosure), or qualifies for a delay of automatic declassification in accordance with paragraph 12.g. of this section, the documents shall be declassified.

(1) Documents not reviewed by December 31 of the year in which they become 25 years old shall be automatically declassified unless the onset of automatic declassification has been delayed in accordance with paragraph 12.g. of this section or an exemption has been approved.

(2) Documents exempted from declassification shall be automatically declassified on December 31 of the year in which they become 50 years old or, as appropriate, 75 years old unless further exempted from declassification in accordance with section 13 of this enclosure.

(3) If the document's date of origin cannot be readily determined, the date of original classification shall be used to determine the automatic declassification deadline.

b. Secretary of Defense Certification. In addition to the requirement of paragraph 12.a. of this section, DoD Components shall not automatically declassify DoD records without reviewing them for declassification unless the Secretary of Defense has certified to Congress that such declassification would not harm the national security pursuant to section 1041 of Public Law 106-65 (Reference (bc)). If records will not be reviewed for declassification as required prior to December 31 of the year in which they become 25 years old, the DoD Component Heads shall notify the USD(I), 6 months in advance of the deadline, so the required Secretary of Defense certification can be addressed. Notification shall include identification of the records, the compelling reason why the records will not be reviewed by the deadline, how many records will remain unreviewed, where the records are located, and when the required reviews will be completed.

c. Public Release of Automatically Declassified Documents. Automatic declassification does not constitute approval for public release of the information. Automatically declassified documents shall not be released to the public until a public disclosure review has been conducted in accordance with paragraph 1.e. of this enclosure. Declassified information may be designated CUI in accordance with Volume 4 of this Manual if it meets the criteria for designation; information so designated shall be marked and protected as Volume 4 requires.

d. Basis for Exclusion or Exemption from Automatic Declassification. Information shall be excluded or exempted from automatic declassification provisions based on content. Exclusion or exemption shall not be based solely on the type of document or record in which the information is found.

e. Exclusion of RD and FRD. Documents and other materials marked or containing RD or FRD are excluded from the automatic declassification provisions of Reference (d) and this Volume until the RD or FRD designation is properly removed. Such information shall remain classified or shall be referred for a declassification review to the Department of Energy if RD or the DASD(NM) if FRD.

(1) In accordance with the provisions of section 3161 of Public Law 105-261 (Reference (bd)) (also known as “The Kyl-Lott Amendment”), and its implementing plan, all personnel who perform automatic declassification reviews on records that are highly likely to contain RD or FRD must be trained and certified by the Department of Energy in the identification of unmarked RD and FRD information. DoD Components shall report each confirmed inadvertent release of RD or FRD occurring during declassification processes to the Department of Energy and provide a copy to OUSD(I) Security Directorate.

(2) When the RD or FRD pertains to defense nuclear information, declassification reviews shall be referred to the DASD(NM), who has OCA for defense nuclear information, to include joint OCA with the Department of Energy for FRD.

(3) The Secretary of Energy determines when information concerning foreign nuclear programs that was removed from the RD category in order to carry out provisions of section 2673 of Reference (ac) may be declassified. Unless otherwise determined by the appropriate OCA, such information shall be declassified when comparable information concerning the U.S. nuclear program is declassified.

f. Integral File Block. Classified records within an integral file block that are otherwise subject to automatic declassification in accordance with this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the MOST RECENT record or the date specified by the exemption instruction of the most recent exempted record, whichever is later, within the file block. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

g. Delays of Automatic Declassification. The following lists the scenarios for which automatic declassification may be delayed.

(1) Media That Is Difficult or Costly to Review. Before the records are subject to automatic declassification, a DoD Component Head or senior agency official may delay automatic declassification for up to 5 additional years for classified information contained in media that make a review for possible declassification more difficult or costly. Prior to taking such action, officials shall consult with the NDC Director, either through the Component declassification plan or by memorandum. The Heads of the Military Departments or their senior agency official shall consult with the NDC Director directly and provide an information copy to the Deputy Under Secretary of Defense Intelligence and Security (DUSD(I&S)). Other DoD Component Heads or their senior agency official shall consult with the NDC Director through DUSD(I&S).

(a) When determined by NARA or jointly determined by NARA and the Department of Defense, automatic declassification may be delayed for:

1. Records requiring extraordinary preservation or conservation treatment, to include reformatting, to preclude damage to the records by declassification processing.

2. Records that pose a potential menace to health, life, or property due to contamination by a hazardous substance.

3. Electronic media if the media is subject to issues of software or hardware obsolescence or degraded data.

(b) Information contained in such media that has been referred shall be automatically declassified 5 years from the date of notification or 30 years from the date of origination of the media, whichever is longer, unless the information has been properly exempted.

(2) Newly Discovered Records. The Director, ISOO, must be consulted whenever a DoD Component Head determines there is a need to delay automatic declassification for newly discovered records that were inadvertently not reviewed prior to the effective date of automatic declassification. Such consultation shall occur not later than 90 days from discovery of the records. Heads of the Military Departments or their senior agency official will notify ISOO directly and provide an information copy to DUSD(I&S). Other DoD Component Heads or their senior agency official will notify ISOO through the DUSD(I&S). The notification should identify the records and their volume, explain the circumstances leading to discovery of the missed records, and provide the anticipated date for declassification. A DoD Component has up to 3 years from the date of discovery to make a declassification, exemption, or referral determination. Referral to other DoD Components or Federal entities with identified interests or equities shall be in accordance with subparagraph 12.g.(3) and section 15 of this enclosure.

(3) Referred Records

(a) Referring Other Agency Information. Other than records that are properly excluded or exempted from automatic declassification, records containing classified information originated by another department or agency or the disclosure of which would affect the interests or activities of other departments or agencies with respect to the classified information and that could reasonably be expected to fall under one or more of the exemptions identified in paragraph 13.b. of this enclosure shall be identified prior to onset of automatic declassification for later referral to those departments or agencies. DoD Components shall identify other agency information for referral during the initial review of Component records; referral review will take place under the auspices of the NDC or JRC. The records shall be referred using SF 715, "U.S. Government Declassification Review Tab."

(b) Referrals to the Department of Defense. Other agency records subject to automatic declassification that contain defense information shall be reviewed by the appropriate DoD Component upon referral. If a final determination is not provided within 1 year on a

referral made by the NDC, defense information in the referred records shall be automatically declassified.

(c) DoD Component Referrals to Other DoD Components. Records containing information originated by another DoD Component or the disclosure of which would affect the interests or activities of another DoD Component with respect to the classified information shall be referred and processed through the NDC or the JRC, as appropriate. The DoD Component shall be notified of these types of referrals.

(d) Referral Review Period. If any disagreement arises between the JRC and the NDC regarding the referral review period, the JRC shall notify ISOO and USD(I) of the disagreement. In such cases, the Director of ISOO shall determine the appropriate review period for referred records. Otherwise, the JRC shall provide a final determination on referrals received through the NDC within 1 year of referral or the information shall be automatically declassified. If any disagreement arises between the DoD Components regarding the referral review period, the JRC, under the auspices of the USD(I), shall determine the appropriate period of review for the referred records.

h. Automatic Declassification of Backlogged Records at NARA. In accordance with Presidential Memorandum (Reference (be)) and under NDC direction:

(1) Referrals and quality assurance problems within the backlog of more than 400 million pages of accessioned Federal records previously subject to automatic declassification shall be addressed in a manner that will permit public access to all declassified records from this backlog no later than December 31, 2013.

(2) DoD Components shall review all referrals to DoD in the backlogged records and identify potentially exemptible information for further referral to other agencies. For DoD, the backlog includes all records reviewed for automatic declassification from April 1995 to December 2009 that have been accessioned, but not processed, by NARA.

i. Declassification Review Technique. DoD Components may use a pass/fail or a redaction declassification technique when doing automatic declassification reviews.

13. EXEMPTIONS FROM AUTOMATIC DECLASSIFICATION. Reference (d) sets out three types of exemptions, specific criteria and duration, and the requirements for requesting an exemption from automatic declassification. Information not exempted from automatic declassification shall be automatically declassified no later than December 31 of the year that is 25 years from the date of origin. Information exempted from automatic declassification remains subject to the mandatory and systematic declassification review provisions of this Volume.

a. Exemption Types

(1) Specific Information. This exemption option permits OCAs to identify and select specific information that should be exempted from the automatic declassification provisions.

The information is described topically in a manner similar to how topics of information are described in a security classification guide and must fall within one or more of the exemption categories described in paragraph 13.b. of this section.

(2) Specific Records. This exemption option permits OCAs to identify and select specific records for exemption from the automatic declassification provisions. The records must be described at the records title level and must contain information that is eligible for exemption under one or more of the exemption categories described in paragraph 13.b. of this section.

(3) File Series. This exemption option allows OCAs to identify an entire file series that should be exempted from the automatic declassification provisions. File series shall be considered for exemption only after a review or assessment has determined that the series is replete with information that almost invariably falls within one or more of the exemption categories described in paragraph 13.b. of this section.

b. Exemption Criteria and Duration

(1) Exempting 25-Year-Old Information. Information that is 25 years old may be exempted (by topic or file series) from automatic declassification for a period not to exceed 50 years from the date of origin when the release would clearly and demonstrably be expected to:

(a) Reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development (exemption 25X1);

(b) Reveal information that would assist in the development, production, or use of weapons of mass destruction (exemption 25X2);

(c) Reveal information that would impair U.S. cryptologic systems or activities (exemption 25X3);

(d) Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system (exemption 25X4);

(e) Reveal formally named or numbered U.S. Military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans (exemption 25X5);

(f) Reveal information, including FGI, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States (exemption 25X6);

(g) Reveal information that would impair the current ability of U.S. Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized (exemption 25X7);

(h) Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security (exemption 25X8); or

(i) Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years (exemption 25X9).

(2) Exempting 50-Year-Old Information. Information that is 50 years old may continue to be exempted (by topic or files series) from automatic declassification for an additional 25 years (i.e., for a period not to exceed 75 years from the date of origin) when:

(a) The release would clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source (exemption 50X1-HUM), or key design concepts of weapons of mass destruction (exemption 50X2-WMD), or

(b) In extraordinary cases, the Secretary of Defense or the Secretary of a Military Department, or their senior agency officials, as appropriate, proposes within 5 years of the onset of automatic declassification to further exempt specific information from declassification at 50 years. The exemption category numbers are the same as for 25 year exemptions, except the number "50" shall be used in place of "25."

(3) Exempting 75-Year-Old Information. The Secretary of Defense or the Secretaries of the Military Departments, or their senior agency officials, as appropriate, may propose within 5 years of the onset of automatic declassification to further exempt specific information from declassification at 75 years. Such proposals must be formally accepted by the ISCAP. The exemption category numbers are the same as for 25 year exemptions, except the number "75" shall be used in place of "25."

(4) File Series Exemptions Approved Prior to December 31, 2008. File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional DoD Component action pending ISCAP review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

(5) Declassification of 50-Year-Old Information in Previously Exempted Records. All previously exempted records, both file series and specific information, that are 50 years or older as of December 31, 2012, shall be automatically declassified by that date unless further exempted in accordance with subparagraphs 13.b.(2) through 13.b.(4) of this section. All existing records meeting the criteria shall be processed for declassification by December 31, 2012. Declassification actions shall be accomplished in accordance with the schedule and priority issued by the NDC. After December 31, 2012, previously exempted records shall be automatically declassified on December 31 of the year that is no more than 50 years from the date of origin unless further exempted in accordance with this section.

c. Exemption Requests. Requests for exemption shall include all information necessary for making a decision. Requests to extend the duration of an exemption shall be processed in the same manner as an initial request.

(1) Requesting an Exemption for Specific Information or Specific Records. OCAs shall provide the following information:

- (a) A detailed description of the information, in the form of a declassification guide.
- (b) An explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time.
- (c) A specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption. The date or event shall not exceed December 31 of the year that is 50 years from the date of origin of the records (75 years for 50 year old material), except a date or event is not required when the information identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction.
- (d) If appropriate, a statement that the exemption will be cited subsequently in applicable classification guides to provide declassification guidance.
- (e) If requesting an exemption from declassification at 50 or 75 years, a statement of support from the USD(I), as the designee of the Secretary of Defense. DoD Components that are elements of the Intelligence Community shall also provide a statement of support from the DNI.

(2) Requesting an Exemption for a File Series. OCAs shall provide the following information:

- (a) A description of the file series.
- (b) An explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time.
- (c) A specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records (75 years for 50 year old information), except a date or event is not required when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction.
- (d) If appropriate, a statement that the exemption will be cited subsequently in applicable classification guides to provide declassification guidance.

(e) If requesting an exemption from declassification at 50 or 75 years, a statement of support from the USD(I), as the designee of Secretary of Defense. DoD Components that are elements of the Intelligence Community shall also provide a statement of support from the DNI.

d. When to Request an Exemption. Exemptions shall be requested not more than 5 years and not less than 1 year before information is subject to automatic declassification except for 75-year exemptions which shall be requested in accordance with subparagraph 13.b.(3) of this section.

e. Who Identifies and Requests an Exemption. In all cases, OCAs are responsible for identifying information that should be exempted from automatic declassification. The type of exemption requested (i.e., specific information, specific records, or file series) determines who must request the exemption.

(1) Specific Information and Specific Records. The senior agency official of a Military Department or the USD(I) acting as the DoD senior agency official, as appropriate, requests exemptions for specific information and specific records from automatic declassification. OCAs, except those in a Military Department, shall request exemptions for specific information and specific records through their DoD Component Head to USD(I). USD(I) shall notify the Director of ISOO, serving as Executive Secretary of the ISCAP, of any information or records that the Component proposes to exempt from automatic declassification. OCAs within a Military Department shall request exemptions through their Department's senior agency official, who shall notify the Director of ISOO and provide USD(I) an information copy for oversight purposes.

(2) File Series. For file series exemptions, the Secretary of Defense or the Secretary of a Military Department, as appropriate, must request the exemption. In either case, the request is forwarded to the Director of ISOO, serving as Executive Secretary of the ISCAP. OCAs, except those within a Military Department, shall submit requests for file series exemption through their DoD Component Head to USD(I). USD(I) will forward the request to the Secretary of Defense for decision and ISCAP notification. OCAs within the Military Departments shall submit requests for exemption to the Secretary of the Military Department, who shall notify the ISCAP. Military Departments shall provide USD(I) an information copy of such notifications for oversight purposes.

f. ISCAP Authority. The ISCAP may direct the Department of Defense not to exempt the specific information, specific records, or file series, or to declassify it at an earlier date than recommended. The Secretary of Defense or the Secretary of a Military Department, as appropriate, may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending. OCAs shall notify the appropriate DoD authority if an appeal is necessary and provide justification and rationale to counter the ISCAP decision. Military Departments shall provide USD(I) an information copy of any appeal for oversight purposes.

g. Notice to Information Holders. When information has been approved for exemption by the ISCAP, the OCA must notify all known information holders. This may be done through

issuance of a memorandum or distribution of the declassification guide. DoD Components that have ISCAP-approved declassification guides must ensure maximum dissemination to record holders of the information. Holders shall re-mark documents in their possession to reflect the exemption.

14. DECLASSIFICATION OF INFORMATION MARKED WITH OLD DECLASSIFICATION INSTRUCTIONS

a. In accordance with Reference (f), when information is marked with previously authorized exemption categories X-1 through X-8, or with the instructions “OADR” (Originating Agency’s Determination Required) or “MR” (Manual Review), including when preceded by “Source marked,” use a declassification date of 25 years from the date of the source document or 25 years from the current date if the source document date is not available, unless exempted in accordance with section 13 of this enclosure.

b. If imagery subject to E.O. 12951 (Reference (bf)) is marked with the declassification instruction “DCI Only” or “DNI Only,” use “25X1, E.O. 12951” as the declassification instruction, as specified by the DNI. (Contact the National Geospatial-Intelligence Agency, Classification Management (NGA/SISX) for assistance in determining whether specific imagery is subject to E.O. 12951.) Otherwise, for documents marked with the declassification instructions “DCI Only” or “DNI Only” which do NOT contain information subject to Reference (bf), use a declassification date that is 25 years from the date of the source document or 25 years from the current date if the source document date is not available.

15. REFERRALS IN THE AUTOMATIC DECLASSIFICATION PROCESS. Referrals are required by References (d) and (f) to ensure timely, efficient, and effective processing of reviews and to protect classified information from inadvertent disclosure. All referrals contained within accessioned records will be processed through the NDC or JRC.

a. Description. The referral process involves identification of information in records containing classified information that originated with another DoD Component or Executive Branch agency or the disclosure of which would affect the interests or activities of another DoD Component or Executive Branch agency and that could reasonably be expected to fall within one or more of the exemptions listed in subparagraph 13.b.(1) of this enclosure. Such records are eligible for referral. The referral process also requires formal notification of referral, making the records available for review, and recording final determinations.

b. Referral Responsibility. Identification of records eligible for referral is the responsibility of the primary reviewing agency and shall be completed prior to the date for automatic declassification established in accordance with section 12 of this enclosure. DoD Components shall use SF 715 to identify any record requiring referral.

16. MANDATORY DECLASSIFICATION REVIEW. Any individual or organization may

request a declassification review of information classified pursuant to Reference (d) or previous classified national security information orders. Heads of the DoD Components shall establish processes for responding to such requests in accordance with Reference (f).

a. Information reviewed shall be declassified if it no longer meets the standards for classification established by this Volume. The declassified information shall be released unless withholding is authorized under other applicable law and the requirement of paragraph 1.e. of this enclosure.

b. Upon receiving a request for a mandatory declassification review, the responsible DoD organization shall conduct the review if:

(1) The request describes the document or material with enough specificity to allow DoD Component personnel to locate the records with a reasonable amount of effort. Requests for broad types of information, entire file series of records, or similar non-specific requests may be denied.

(2) The information falls under its purview.

(a) If documents or material being reviewed for declassification contain information originally classified by another DoD Component or U.S. Government agency or the disclosure of which would affect the interests or activities of another DoD Component or U.S. Government agency, the reviewing activity shall refer the appropriate portions of the request to the originating or affected organization. Unless the association of that organization with the requested information is itself classified, the DoD Component that received the review request shall notify the requester of the referral. The DoD Component that received the review request remains responsible for collecting all determinations made by organizations to which the information was referred and for informing the requestor of the final decision regarding declassification, unless other prior arrangements have been made.

(b) Requests for cryptologic information shall be processed in accordance with section 7 of this enclosure.

(c) The DoD Component that initially received or classified FGI shall determine whether the information is subject to a treaty or international agreement that does not permit unilateral declassification. (Refer also to section 20 of this enclosure.)

(3) The information is not the subject of pending litigation.

(4) The information is not contained within an operational file that is exempt from search and review, or disclosure, pursuant to sections 431, 432, 432a and 432b of Reference (ac) or other applicable statute.

(5) The information has not been reviewed for declassification within the preceding 2 years. If the requested information has been reviewed for declassification within the 2 years

preceding the request, the DoD Component shall notify the requester of the prior review decision and provide appeal rights information. No further review is required.

(6) The information was not originated by the incumbent President or the incumbent Vice President, the incumbent President's White House staff, or the incumbent Vice President's staff, committees, commissions, or boards appointed by the incumbent President, or other entities within the Executive Office of the President that solely advise and assist the incumbent President. Information so originated is exempt from the provisions of this section.

(7) The request was submitted to a Defense Intelligence Component by a U.S. citizen or an alien lawfully admitted for permanent residence; otherwise, the request may be denied.

c. A DoD Component may refuse to confirm or deny the existence or nonexistence of requested information when the fact of its existence or nonexistence is properly classified.

d. DoD Components shall either make a prompt declassification determination and notify the requester accordingly, or inform the requester of the additional time needed to process the request. DoD Components shall ordinarily make a final determination within 1 year from the date of receipt.

(1) In making a declassification determination DoD Components shall determine whether the information continues to meet the requirements for classification. Information to be withheld must not only qualify for classification under the criteria identified in paragraph 1.b of Enclosure 4, but there also must be a current basis for continued classification.

(2) When information cannot be declassified in its entirety, DoD Components shall make reasonable efforts to release, consistent with other applicable law and the requirements of paragraph 1.e. of this enclosure, those declassified portions of the requested information that constitute a coherent segment. Where information is withheld the specific reason, as specified by section 1.4 of Reference (d) and identified in paragraph 1.b of Enclosure 4 of this Volume, must be included for each redaction. Information that is redacted due to a statutory authority must be clearly marked with the specific authority that authorizes the redaction.

e. The mandatory declassification review process shall provide for administrative appeal in cases where the review results in the information remaining classified. The requester shall be notified of the results of the review and of the right to appeal, within 60 days of receipt, the denial of declassification. If the requester files an appeal, the DoD Component appellate authority shall make a determination within 60 working days following receipt. If additional time is required to make a determination, the appellate authority shall notify the requester of the additional time needed and provide the reason for the extension. If the appeal is denied, the requester shall be notified of the right to appeal the denial to the ISCAP.

f. Requesters may be charged fees for processing their requests in accordance with the schedule of fees in Volume 11 A of DoD 7000.14-R (Reference (bg)).

17. SYSTEMATIC REVIEW FOR DECLASSIFICATION. Heads of the DoD Components that have classified information in accordance with Reference (d) or previous Executive orders shall establish systematic review programs to review for declassification information in the custody of the DoD Component. These programs shall review for declassification information that is contained in permanently valuable historical records that have been exempted from automatic declassification and shall determine if the information may be further exempt from automatic declassification in accordance with the provisions of this enclosure. These efforts shall be prioritized in accordance with the priorities established by the NDC.

18. DOWNGRADING CLASSIFIED INFORMATION. Downgrading information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level and can be properly protected at a lower level. The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level. Any official with jurisdiction over the information who is authorized to classify or declassify the information may downgrade it.

a. Downgrading shall be considered when OCAs are deciding on the duration of classification to be assigned. If downgrading dates or events can be identified, they shall be specified along with the declassification instruction. Downgrading instructions do not replace declassification instructions.

b. An authorized official making a downgrading decision shall notify all known holders of the change in classification. If the information is subject to the Scientific and Technical Information Program (STIP) (DoDD 3200.12 (Reference (bh))), the authorized official shall also notify DTIC.

c. When information is marked for downgrading on a specific date or event and that date or event has passed, holders shall confirm that the OCA(s) of the information has not extended the higher classification period prior to downgrading DoD information.

d. Downgraded information shall be marked as required by Enclosure 3 of Volume 2 of this Manual.

e. If a holder of classified information has reason to believe it should not be downgraded as indicated, the originator shall be notified through appropriate administrative channels. The document or material shall continue to be protected at the originally assigned classification until the issue is resolved.

19. UPGRADING CLASSIFIED INFORMATION. Classified information may be upgraded to a higher level of classification only by officials who have been delegated the appropriate level of original classification authority in accordance with Enclosure 4 of this Volume. The information to be upgraded must continue to meet the standards for classification specified in Enclosure 4 of this Volume. When making the decision to upgrade the classification level, OCAs shall consider the benefits to national security that will accrue from the higher classification against the costs

associated with upgrading (e.g., the requirement for upgraded clearances or storage facilities, notification costs) and the ability to notify all holders of the information of the change so that the information shall be uniformly protected at the higher level. The OCA making the upgrading decision is responsible for notifying holders of the change in classification. For information subject to the STIP (Reference (bh)), the OCA shall also notify DTIC. Upgraded information shall be marked as required by Enclosure 3 of Volume 2 of this Manual.

20. DECLASSIFYING FGI. Pursuant to Reference (d), FGI qualifies as an exemption to the automatic declassification rule. Within the Department of Defense, every effort shall be made to ensure that FGI is not subject to downgrading or declassification without the prior consent of the originating government. FGI may exist in two forms: foreign documents in possession of the Department of Defense, and foreign government classified information included within U.S. Government documents.

a. If FGI in the form of foreign documents in the possession of the Department of Defense constitute permanently valuable records of the U.S. Government and are subject to the 25-year automatic declassification rule, declassification officials shall consult with the originating foreign government to determine whether it consents to declassification. If the originating foreign government does not consent, the records shall be processed for exemption from automatic declassification in accordance with section 13 of this enclosure. The agency head shall determine whether exemption category 25X6, 25X9, or both should be applied.

b. U.S. Government documents that include classified FGI shall be marked with declassification instructions as specified in this enclosure and Volume 2 of this Manual. If these documents are permanently valuable records of the U.S. Government and are subject to the 25-year automatic declassification rule, the provisions of paragraph 20.a. of this section shall apply. A U.S. document marked as described herein cannot be downgraded below the highest level of FGI contained in the document or be declassified without the written permission of the foreign government or international organization that originated the information. Submit recommendations concerning downgrading or declassification to the DoD organization that created the document. If that organization supports the recommendation, it shall consult with the originating foreign government to determine whether that government consents to declassification.

c. DoD officials may consult directly with foreign governments regarding downgrading or declassification of FGI or seek assistance from the Department of State. In either case, DoD officials should first consult with the Director, International Security Programs, Defense Technology Security Administration, OUSD(P), for assistance and guidance.

21. APPLICATION OF DECLASSIFICATION AND EXTENSION OF CLASSIFICATION TO PRESENT AND PREDECESSOR EXECUTIVE ORDERS. The requirements for declassifying and extending classification specified by this enclosure apply to information classified in accordance with E.O. 12958 (Reference (bi)) and earlier Executive orders, as well as to information classified pursuant to Reference (d).

ENCLOSURE 6

SECURITY CLASSIFICATION GUIDES

1. GENERAL. Reference (d) requires issuance of classification guidance to facilitate proper and uniform derivative classification of information. Issuance of timely and precise classification guidance by the responsible OCA is a prerequisite to effective and efficient information security and assures that security resources are expended to protect only that information warranting protection in the interests of national security.

a. The responsible OCA shall issue a security classification guide for each system, plan, program, or project involving classified information and shall ensure it is reviewed and updated as provided by this enclosure. DoD 5200.1-H (Reference (bj)) provides guidance to assist in development of a security classification guide.

b. A security classification guide shall be issued as early as practical in the life cycle of the system, plan, program, or project, preferably prior to release of information regarding the system, plan, program, or project.

c. When possible, OCAs should communicate with others who are responsible for classification guidance for similar activities to ensure consistency and uniformity of classification decisions. Additionally, when possible OCAs should seek user input when reviewing guides for revision.

d. A security classification guide shall be classified by the approving OCA if it meets the requirement for being classified. If the guidance does not warrant classification, it shall be marked and protected as For Official Use Only (FOUO). Security classification guides shall not be released to the public nor posted on publicly accessible websites. If requested in accordance with FOIA, the section of the security classification guide that addresses the specific items to be classified, including the reasons for classification, shall be denied pursuant to exemption (b)(2) of the FOIA.

2. CONTENT OF SECURITY CLASSIFICATION GUIDES. Security classification guides shall:

a. Identify specific items or elements of information to be protected.

b. State the specific classification assigned to each item or element of information. Where an item or element of information may qualify for one of multiple classification levels (e.g., Unclassified to Secret), criteria must be provided for determining which classification level is applicable. Simply citing a range is not permissible.

c. State a concise reason for classifying each item, element, or category of information and cite the applicable classification category(ies) in section 1.4 of Reference (d).

d. State the declassification instructions for each item or element of classified information, including citation of the approved automatic declassification exemption category, if any.

(1) For information exempted from automatic declassification because disclosing it may reveal FGI or violate a statute, treaty, or international agreement (see subparagraphs 13.b.(1)(f) and 13.b.(1)(i) of Enclosure 5 of this Volume), the guide shall identify the government or specify the applicable statute, treaty, or international agreement as appropriate.

(2) Automatic declassification exemptions (25X1-25X9) authorized in accordance with section 13 of Enclosure 5 of this Volume may be cited in classification guides for use on derivatively classified documents once the declassification guide has been submitted to the ISCAP. The ISCAP must be notified in advance of the declassification guide's approval of the intent to cite such exemptions in applicable classification guides (refer to paragraph 13.c. of Enclosure 5 of this Volume), and the information being exempted must remain in active use.

(3) Where applicable, the security classification guide should refer to the declassification guide for specific declassification guidance.

e. Identify any special handling caveats (e.g., dissemination controls) that apply to items, elements, or categories of information. Where applicable, use remarks or a releasability annex to identify those elements of information approved, in accordance with established disclosure policies, by the appropriate disclosure authority(s) for routine release to specified foreign governments and international organizations.

f. Identify, by name or personal identifier and position title, the original classification authority approving the guide and the date of approval.

g. Provide a point of contact for questions about the guide and suggestions for improvement.

3. CUI AND UNCLASSIFIED ELEMENTS OF INFORMATION. OCAs and developers of security classification guides are encouraged to specify in security classification guides specific items or elements of unclassified information or CUI to be protected. Cite the appropriate classification (e.g., (U)) or CUI designation (e.g., FOUO), and identify any special handling caveats (e.g., export controls) that apply. FOUO information is information that should be withheld from the public because of foreseeable harm to an interest protected by the FOIA, as implemented by DoD 5400.7-R (Reference (bk)). See Volume 4 of this Manual for further information on CUI.

4. DATA COMPILATION CONSIDERATIONS. Posting of unclassified defense and U.S. Government information to publicly accessible Internet sites makes access to the information from anywhere in the world easy and affordable. Search capabilities and data mining tools make discovery and correlation of available information fast and simple. This ability to discover and analyze militarily-relevant data creates the need to pay particular attention to classified

compilations of data elements. Where specific combinations of unclassified data elements are known to be classified, CONSISTENTLY withholding specified data elements from public Internet posting and, to the extent possible consistent with statute and other regulations, public release can mitigate the ability of others to create the classified compilation. Thus, OCAs should consider including in security classification guides, where appropriate, prohibitions on posting one or more of the specific data elements that are known to make up a classified compilation of unclassified data elements to publicly accessible Internet sites. See section 15 of Enclosure 4 for guidance on classification by compilation.

5. APPROVAL OF SECURITY CLASSIFICATION GUIDES. An OCA shall personally approve, in writing, security classification guides. This OCA shall be an official who:

a. Has program or supervisory responsibility for the information, or is the senior agency official for Department of Defense or for the originating Military Department.

b. Is authorized to originally classify information at the highest level the guide specifies.

6. DISTRIBUTION OF SECURITY CLASSIFICATION GUIDES. The originating organization shall:

a. Distribute security classification guides to those organizations and activities that may classify information the guide covers.

b. Forward one copy of each guide (including those issued as regulations, manuals, or other Component issuances) to the Office of Security Review, Washington Headquarters Service. Guides that cover SCI or SAP information and that contain information that requires special access controls are exempt from this requirement. The mailing address to use is:

Department of Defense
Office of Security Review
1155 Defense Pentagon
Washington, DC 20301-1155

c. Provide one copy of each approved guide (including those issued as regulations, manuals, or other issuances, but not those covering Top Secret, SCI or SAP information, or guides deemed by the guide's approval authority to be too sensitive for automatic secondary distribution) to the Administrator, DTIC, along with DD Form 2024. Each guide furnished to DTIC shall bear the appropriate distribution statement required by Reference (aj). (See also Enclosure 3 of Volume 2 for guidance on distribution statements.) DTIC's mailing address is:

Defense Technical Information Center
ATTN: DTIC-OA (Security Classification Guides)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

For information on e-mail or electronic submission, contact TR@dtic.mil.

- d. Provide one copy of each approved guide to the activity security manager.
- e. Provide one copy to the DoD Component declassification program manager.

7. INDEX OF SECURITY CLASSIFICATION GUIDES. Security classification guidance (e.g., security classification guides, memorandums, directives, regulations) issued in accordance with this enclosure shall be indexed in an on-line accessible database maintained by DTIC. Originators of guides shall submit DD Form 2024 to the Administrator, DTIC, upon approval of the guide, with each update, revision, or review, or whenever the guide is cancelled or superseded. If the originator determines that listing the guide in the DTIC-maintained database is inadvisable for security reasons (e.g., involves SAPs), the originator shall separately report issuing the guide to the Director of Security, OUSD(I), and explain why the guide should not be listed.

8. REVIEW OF SECURITY CLASSIFICATION GUIDES. Each security classification guide shall be reviewed by the issuing OCA at least once every 5 years to ensure it is current and accurate. When necessitated by significant changes in Executive orders or by changes in operations, plans, or programs, reviews will be conducted sooner. The OCA shall make changes identified as necessary in the review process. If no changes are required, the OCA shall submit to DTIC a new DD Form 2024 with the date of the next required review and annotate the record copy of the guide with this fact and the date of the review.

9. REVISION OF SECURITY CLASSIFICATION GUIDES. Guides shall be revised whenever necessary to promote effective derivative classification. Revised guides shall be reported as required in section 7 of this enclosure.

10. CANCELLING SECURITY CLASSIFICATION GUIDES

a. Guides shall be canceled only when:

- (1) All information the guide specifies as classified has been declassified; or
- (2) A new security classification guide incorporates the classified information covered by the old guide and there is no reasonable likelihood that any information not incorporated by the new guide shall be the subject of derivative classification. The impact on systems, plans, programs, or projects must be considered when deciding to cancel a guide.

b. Upon canceling a guide, the responsible official shall consider the need for publishing a declassification guide, according to section 4 of Enclosure 5.

c. The OCA, or successor organization, shall maintain a record copy of any canceled guide as required by Reference (at).

11. REPORTING CHANGES TO SECURITY CLASSIFICATION GUIDES. Revision, reissuance, review, supersession, and cancellation of a guide shall be reported to DTIC using DD Form 2024, according to section 7 of this enclosure. Copies of changes, reissued guides, and cancellation notices will be distributed according to section 6 of this enclosure.

12. FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEWS. As periodically directed by the USD(I), but at least every 5 years, the DoD Component Heads shall accomplish comprehensive reviews of classification guidance issued by the DoD Component.

a. Reviews shall ensure the DoD Component's classification guidance reflects current conditions. The reviews shall also identify classified information that no longer requires protection and can be declassified.

b. Reviews shall focus on a review of security classification guides, but should consider all forms of classification guidance issued (e.g., memorandums, DoD Component regulation or directive).

c. Reviews shall include an evaluation of classified information to determine if it continues to meet the standards for classification specified in section 1 of Enclosure 4 of this Volume, using a current assessment of likely damage.

d. OCAs, DoD Component subject matter experts, and users of the classification guidance shall be consulted to provide a broad range of perspectives. Contributions of subject matter experts with sufficient expertise in narrow specializations must be balanced by the participation of managers and planners who have broader organizational vision and relationships. Additionally, to the extent practicable, input should also be obtained from external subject matter experts and external users of the classification guidance.

e. Detailed reports summarizing results and findings shall be prepared and submitted in accordance with the direction provided and shall be unclassified and releasable to the public, except when the existence of the guide or program is itself classified. OUSD(I) shall provide a composite DoD report to ISOO and release an unclassified version to the public.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ACCM	alternative compensatory control measures
B&P	bid and proposal
CI	counterintelligence
CNWDI	Critical Nuclear Weapon Design Information
COMSEC	communication security
CUI	controlled unclassified information
CUIO	Controlled Unclassified Information Office
CUSR	Central U.S Registry
DAA	designated approval authority
DASD(NM)	Deputy Assistant Secretary of Defense for Nuclear Matters
DD	DoD
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoDD	DoD Directive
DoD CIO	DoD Chief Information Officer
DoDI	DoD Instruction
DSS	Defense Security Service
DTIC	Defense Technical Information Center
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence and Security
E.O.	Executive order
FGI	foreign government information
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRD	Formerly Restricted Data
GS	General Schedule
IA	information assurance
IAM	information assurance manager
IR&D	independent research and development
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
IT	information technology
JRC	Joint Referral Center

MR	manual review
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NC2-ESI	Nuclear Command and Control-Extremely Sensitive Information
NDC	National Declassification Center
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
OADR	originating agency's determination required
OCA	original classification authority
OPSEC	operations security
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OUSD(P)	Office of the Under Secretary of Defense for Policy
RD	Restricted Data
SAP	Special Access Program
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SF	standard form
SIPRNET	Secret Internet Protocol Router Network
SSO	special security officer
STIP	Scientific and Technical Information Program
TSCA	Top Secret control assistant
TSCO	Top Secret control officer
UCMJ	Uniform Code of Military Justice
U.S.C.	United States Code
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USSAN	United States Security Authority for NATO
WHS	Washington Headquarters Services

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Volume.

access. The ability or opportunity to obtain knowledge of classified information.

accessioned records. Records of permanent historical value in the legal custody of NARA.

activity security manager. The individual specifically designated in writing and responsible for the activity's information security program, which ensures that classified information (except SCI which is the responsibility of the SSO appointed by the senior intelligence official) and CUI are properly handled during their entire life cycle. This includes ensuring information is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken. The security manager may be assigned responsibilities in other security disciplines such as personnel and physical security, etc. The activity security manager implements the information security program guidance established by this Manual and the Component senior agency official.

agency. Any Executive agency as defined in section 105 of Reference (av); any Military Department as defined in section 102 of Reference (av); and any other entity within the Executive Branch that comes into the possession of classified information.

authorized person. A person who has a favorable determination of eligibility for access to classified information, has signed an SF 312 nondisclosure agreement, and has a need to know for the specific classified information in the performance of official duties.

automatic declassification. The declassification of information based solely upon:

The occurrence of a specific date or event as determined by the original classification authority; or

The expiration of a maximum time frame for duration of classification established pursuant to Reference (d).

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

classification guidance. Any instruction or source that prescribes the classification of specific information.

classification guide. A documentary form of classification guidance issued by an OCA that identifies, for a specific subject, the elements of information that must be classified and establishes the level and duration of classification for each such element.

classified national security information. Information that has been determined pursuant to Reference (d), or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

classifier. An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an OCA or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

collateral information. All national security information classified Confidential, Secret, or Top Secret under the provision of an Executive order for which special systems of compartmentation (such as SCI or SAP) are not formally required.

compilation. An aggregation of preexisting items of information.

compromise. An unauthorized disclosure of classified information.

COMSEC. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

confidential source. Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

control. The authority of the agency that originates information, or its successor in function, to regulate access to the information.

CUI. Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

damage to the national security. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

declassification. The authorized change in the status of information from classified information to unclassified information.

declassification authority

The official who authorized the original classification, if that official is still serving in the same position;

The originator's current successor in function, if that individual has original classification authority;

A supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or

Officials delegated declassification authority in writing by the agency head or the senior agency official.

declassification guide. Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified. May also be a guide providing classification and declassification instructions specifically for information that is 25 years old or older and of permanent historical value. A declassification guide is the most commonly used vehicle for obtaining ISCAP approval of 25-year exemptions from the automatic declassification provisions of Reference (d).

Defense Intelligence Components. All DoD organizations that perform national intelligence, Defense Intelligence, and intelligence-related functions, including: the Defense Intelligence Agency; the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency/Central Security Service, and the intelligence elements of the Active and Reserve components of the Military Departments, including the United States Coast Guard when operating as a service in the Navy.

derivative classification. Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

distribution statement. A statement used on a technical document to denote the extent of its availability for secondary distribution, release, and disclosure without additional approvals or authorizations. A distribution statement is distinct from and in addition to a security classification marking and any dissemination control markings included in the banner line. A distribution statement is also required on security classification guides submitted to DTIC.

document. Any recorded information, regardless of the nature of the medium or the method or circumstances of recording. This includes any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage media.

downgrading. A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

element of the Intelligence Community. See Intelligence Community.

equity. For purposes of classification management, information originally classified by or under the control of an agency.

exempted. Nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification in accordance with Reference (d).

FGI

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.

Information produced by the U.S. Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

Information received and treated as FGI pursuant to the terms of a predecessor order to Reference (d).

file series. File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use. Also documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same subject, function, or activity.

file series exemption. An exception to the 25-year automatic declassification provisions of Reference (d). This exception applies to entire blocks of records, i.e., “file series,” within an agency’s records management program. To qualify for this exemption, the file series must be replete with exemptible information.

FOUO. A protective marking to be applied to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more provisions of the FOIA. This includes information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended. See Reference (bk) for detailed information on categories of information that may qualify for exemption from public disclosure.

FRD. Information removed from the RD category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as RD.

heads of DoD activities. Heads, either military or civilian, of organizations, commands, and staff elements subordinate to a DoD Component, with jurisdiction over and responsibility for the execution of the organization’s mission and functions, including its information security program. The official may carry the title of commander, commanding officer, or director, or other equivalent title.

human intelligence source. People who provide intelligence directly; individuals associated with organizations (such as foreign government entities and intelligence services) who willingly share intelligence information with the United States; individuals and organizations who facilitate the

placement or service of technical collection means that could not succeed without their support; and foreign citizens who are identified as of an intelligence interest to the United States with a reasonable expectation that they will provide information or services in the future. Information that may reveal the identities of people upon whom the United States relies for information, access to information, or cooperation leading to obtaining information is considered to potentially reveal human intelligence sources.

information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

information security. The system of policies, procedures, and requirements established in accordance with Reference (d) to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to Executive order, statute or regulation.

integral file block. A distinct component of a file series that should be maintained as a separate unit to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

integrity. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Intelligence Community. An element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Reference (ae).

international program. Any program, project, contract, operation, exercise, training, experiment, or other initiative that involves a DoD Component or a DoD contractor and a foreign government, international organization, or corporation that is located and incorporated to do business in a foreign country.

material. Any product or substance on or in which information is embodied.

national security. The national defense or foreign relations of the United States. National security includes defense against transnational terrorism.

national security system. Defined in section 3542(b)(2) of Reference (as).

need to know. A determination that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

network. A system of two or more computers that can exchange data or information.

newly discovered records. Records that were inadvertently not reviewed prior to the effective date of automatic declassification because the Agency declassification authority was unaware of their existence.

OCA. An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information (i.e., to classify information in the first instance).

original classification. An initial determination that information requires, in the interests of national security, protection against unauthorized disclosure.

pass/fail. A declassification technique that regards information at the full document level. Any exemptible portion of a document may result in exemption (failure) of the entire document. Documents that contain no exemptible information are passed and therefore declassified. Documents that contain exemptible information are failed and therefore exempt from automatic declassification.

permanent records. Any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States. Permanent records include all records accessioned by NARA into the National Archives of the United States and later increments of the same records, and those for which the disposition is permanent on SF 115, "Request for Records Disposition Authority," approved by NARA on or after May 14, 1973.

permanently valuable records. See "records having permanent historical value."

RD. All data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but not data declassified or removed from the RD category pursuant to section 2162 of The Atomic Energy Act of 1954, as amended.

records. The records of an agency and Presidential papers or Presidential records, as those terms are defined in Reference (as), including those created or maintained by a U.S. Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control in accordance with the terms of the contract, license, certificate, or grant.

records having permanent historical value. Records that the Archivist of the United States has determined should be maintained permanently in accordance with Reference (as).

records management. The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management

of agency operations. Within the Department of Defense, records management is implemented by Reference (at).

redaction. For purposes of declassification, the removal of exempted information from copies of a document.

released to the public. Made available to the general public through any publicly accessible media or method.

risk management. The process of identifying, assessing, and controlling risks and making decisions that balance risk with cost and benefits.

safeguarding. Measures and controls that are prescribed to protect classified information.

SAP. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. In the Department of Defense, any DoD program or activity (as authorized in Reference (d)), employing enhanced security measures (e.g., safeguarding, access requirements), exceeding those normally required for collateral information at the same level of classification, shall be established, approved, and managed as a DoD SAP in accordance with Reference (n).

scheduled records. All records that fall under a NARA-approved records control schedule.

SCI. Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of National Intelligence.

security classification guide. A documentary form of classification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

security clearance. A determination that a person is eligible in accordance with the standards of Reference (o) for access to classified information.

self-inspection. The internal review and evaluation of individual DoD Component activities and the DoD Component as a whole with respect to the implementation of the information security program established in accordance with References (b), (d) and (f), and this Manual.

senior agency official. An official appointed by the head of a DoD Component to be responsible for direction, administration, and oversight of the Component's information security program, to include classification, declassification, safeguarding, and security education and training programs, and for the efficient and effective implementation of References (b), (d), (e), and (f) and the guidance in this Manual. Where used in reference to authorities pursuant to section 5.4(d) of Reference (d), this term applies only to the senior agency officials of the Military Departments and of the Department of Defense.

senior intelligence official. The highest ranking military or civilian charged with direct foreign intelligence missions, functions, or responsibilities with a department, agency, component, or element of an Intelligence Community organization. Responsible for direction, administration, and oversight of the organization's SCI program, to include classification, declassification, safeguarding, and security education and training programs for the effective implementation of References (b), (j), and (z) and the guidance in this Manual.

SSO. Individual appointed, in accordance with References (j) and (z), by the senior intelligence official to be responsible for the day-to-day security management, operation, implementation, use, and dissemination of SCI within an activity.

tab. A narrow paper sleeve placed around a document or group of documents in such a way that it is readily visible.

telecommunications. The preparation, transmission, or communication of information by electronic means.

transferred records. Records transferred to agency storage facilities or a Federal records center.

unauthorized disclosure. Communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient.

unscheduled records. Records whose final disposition has not been approved by NARA.

U.S. entity

State, local, or tribal governments.

State, local, and tribal law enforcement and firefighting entities.

Public health and medical entities.

Regional, State, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities.

Private sector entities serving as part of the Nation's critical infrastructure and/or key resources.

violation

Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.

Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of Reference (d), its implementing directives, or this Manual.

Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of Reference (d), Reference (n), or this Manual.

weapons of mass destruction. Any weapon of mass destruction as defined in section 1801(p) of Reference (ac).



Department of Defense MANUAL

NUMBER 5200.01, Volume 2

February 24, 2012

Incorporating Change 3, Effective May 14, 2019

USD(I)

SUBJECT: DoD Information Security Program: Marking of Information

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual (DoDM) to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP). This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526, E.O. 13556, and parts 2001 and 2002 of title 32, Code of Federal Regulations (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume:

(1) Provides guidance for the correct marking of information.

(2) Incorporates and cancels DoD 5200.1-PH, Directive-Type Memorandum (DTM) 04-009, and DTM 05-008 (References (g), (h), and (i)).

2. APPLICABILITY. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

b. Does not alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community (IC) pursuant to policies issued by the DNI. Consistent with Reference (b), SCI shall be safeguarded in accordance with the policies and procedures issued by the DNI, as implemented by Volumes 1-3 of DoDM 5105.21 (References (j), (k), and (l)) and other applicable guidance.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy, in accordance with Reference (b), to:

a. Identify and protect national security information and CUI in accordance with national level policy issuances.

b. Promote information sharing, facilitate judicious use of resources, and simplify management through implementation of uniform and standardized processes.

c. Prescribe, use, and enforce standards for marking all classified national security information, consistent with the requirements of References (d) and (f).


d. Facilitate information sharing by application of restrictive dissemination markings only where clearly warranted.

5. RESPONSIBILITIES. See Volume 1, Enclosure 2.

6. PROCEDURES. See Enclosures 2 through 4.

7. RELEASABILITY. **Cleared for public release.** Available on the Directives Division Website at <https://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE. This Volume is effective February 24, 2012.



Michael G. Vickers
Under Secretary of Defense
for Intelligence

Enclosures

1. References
2. Overview
3. Marking Principles
4. Marking Standard

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....	9
ENCLOSURE 2: OVERVIEW.....	12
MARKING STANDARD.....	12
EXAMPLES	13
WAIVERS INVOLVING MARKING OF CLASSIFIED INFORMATION	13
COVER SHEETS AND CLASSIFICATION LABELS	14
TRIGRAPHS AND TETRAGRAPHS.....	14
REQUESTS FOR OPERATIONAL TETRAGRAPHS.....	15
Process	15
Considerations.....	15
Request Requirements	15
ENCLOSURE 3: MARKING PRINCIPLES	17
MARKING REQUIREMENT.....	17
GENERAL GUIDELINES	17
REQUIRED MARKINGS ON CLASSIFIED DOCUMENTS.....	18
SPECIAL NOTICES	19
BANNER LINES.....	20
PORTION MARKS.....	21
DOD COMPONENT, OFFICE, AND DATE OF ORIGIN.....	23
CLASSIFICATION AUTHORITY BLOCK.....	24
General Requirements.....	24
Original Classification	24
Derivative Classification.....	27
Examples.....	28
USE OF CALCULATED DECLASSIFICATION DATE IN PLACE OF PREVIOUS DECLASSIFICATION INSTRUCTIONS.....	36
MARKINGS FOR CHANGES IN CLASSIFICATION	37
Confirmation of Change	37
Declassification.....	37
Downgrading.....	37
Downgrading or Declassification Earlier Than Scheduled	38
Upgrading	38
Extension of Classification	38
Reclassification	38
Bulk Changes	38
DECLASSIFICATION MARKINGS	39
CLASSIFICATION AS A RESULT OF COMPILATION	40
WORKING PAPERS.....	41
REFERENCES	43

TRANSMITTAL DOCUMENTS	43
BRIEFING SLIDES.....	46
MARKING IN THE ELECTRONIC ENVIRONMENT	48
General Guidance.....	48
E-Mail Messages.....	49
Web Pages.....	51
URLs.....	51
Dynamic Documents.....	52
Bulletin Board Postings and Blogs	53
Wikis.....	53
Instant Messaging, Chat, and Chat Rooms	54
Attached Files	54
SPECIAL TYPES OF MATERIALS	54
General Guidance.....	54
Blueprints, Engineering Drawings, Charts and Maps.....	55
Photographic Media.....	56
Digital Video Discs (DVDs), Video Tapes, Motion Picture Films, and Web Videos.....	57
Sound Recordings	57
Microfilm, Microfiche, and Similar Microform Media.....	57
Removable Electronic Storage Media	58
MARKING FGI.....	59
MARKING REQUIREMENTS FOR TRANSFERS OF DEFENSE ARTICLES TO AUSTRALIA OR THE UNITED KINGDOM WITHOUT AN EXPORT LICENSE OR OTHER WRITTEN AUTHORIZATION.....	60
TRANSLATIONS	60
MARKING DOCUMENTS FOR TRAINING PURPOSES OR AS AN EXAMPLE	60
DISTRIBUTION STATEMENTS.....	61
ENCLOSURE 4: MARKING STANDARD.....	63
OVERVIEW	63
USE OF THE MARKING “NOT RELEASABLE TO FOREIGN NATIONALS” (NOFORN)	65
U.S. CLASSIFICATION MARKINGS.....	66
FGI MARKINGS USED ON NON-U.S. DOCUMENTS	67
General.....	67
NATO Classification Markings.....	68
Documents Marked RESTRICTED or That Are Provided “in Confidence”	69
JOINT CLASSIFICATION MARKINGS.....	70
SCI CONTROL SYSTEM MARKINGS	72
SAP CONTROL MARKINGS	74
ATOMIC ENERGY ACT INFORMATION MARKINGS	76
RD	77
FRD.....	79
CNWDI.....	80
Sigma	81

FGI MARKINGS USED IN U.S. DOCUMENTS	83
DISSEMINATION CONTROL MARKINGS	87
Dissemination Control Markings for Intelligence Information	87
FOUO.....	87
CUI.....	88
Dissemination and Extraction of Originator Controlled (ORCON) Information	88
Authorized For Release To (REL TO).....	90
Display Only	93
OTHER DISSEMINATION CONTROL MARKINGS.....	95
Alternative Compensatory Control Measures (ACCM)	95
Department of State (DoS) Dissemination Control Markings	96
Equivalent Foreign Security Classifications	96
APPENDIXES	
1. DISSEMINATION CONTROL MARKINGS FOR INTELLIGENCE INFORMATION.....	97
2. DOS DISSEMINATION CONTROL MARKINGS	103
GLOSSARY	106
PART I. ABBREVIATIONS AND ACRONYMS	106
PART II. DEFINITIONS.....	108
TABLE	
1. Authorized Distribution Statements.....	62
FIGURES	
1. Examples of Banner Markings.....	20
2. Examples of Portion Markings	22
3. Example of Originally Classified Document.....	26
4. Example of Derivatively Classified Document	28
5. Markings on a Memorandum.....	33
6. Markings on an Action Memorandum	34
7. Markings on a Staff Summary Sheet	35
8. Use of Calculated Declassification Date.....	36
9. Declassification Markings	40
10. Classification as a Result of Compilation.....	42
11. Markings on Working Papers	43
12. Marking References	43
13. Transmittal Documents.....	45
14. Markings on Briefing Slides	47
15. Multiple Source Listing on Briefing Slides	48
16. Marking E-Mails	50
17. Examples of URL with Included Portion Mark.....	52

18. Example of Portion-Marked URL Embedded in Text.....	52
19. Warning Statement for Dynamic Documents	53
20. Markings on Maps	55
21. Markings on Charts.....	56
22. Markings on Photographs	57
23. Markings on IT Systems and Media	59
24. Information Provided by Distribution Statements	61
25. Marking Structure	64
26. Example of U.S. Classification Markings.....	66
27. Example of Markings for Non-U.S. Documents	67
28. Examples of NATO Markings	69
29. CONFIDENTIAL—Modified Handling Example	70
30. Example of Joint Classification Marking	71
31. Example of Joint Classification Marking with REL TO	71
32. Example of Joint Classification Marking in a U.S. Derivative Document.....	72
33. Examples of SCI Control Markings.....	73
34. Examples of SAP Markings.....	75
35. Declassification Markings for SAP Information	75
36. Example of RD Markings	78
37. Example of FRD Markings.....	80
38. Example of CNWDI Markings	81
39. Example of SIGMA Markings.....	82
40. Example of SIGMA 14 Markings.....	83
41. Example of FGI Marking.....	84
42. Example of FGI Marking with NATO Information	84
43. Example of FGI Marking When Originating Country Is Concealed	85
44. Example of FGI Marking with REL TO.....	85
45. Example of FOUO Marking in a Classified Document.....	88
46. Example of ORCON Marking	89
47. Example of REL TO Marking	90
48. Example of REL TO Marking When Not All Portions Are Equally Releasable.....	91
49. Example of REL TO Marking When Portions Lack Explicit Release Markings	92
50. Example of DISPLAY ONLY Marking	93
51. Example of DISPLAY ONLY Marking with REL TO	94
52. Example of Markings When Not All Portions Are DISPLAY ONLY.....	94
53. Example of DISPLAY ONLY Marking in Mixed Releasability Situation	95
54. Example of ACCM Markings.....	96
55. Example of IMCON Marking.....	97
56. Example of IMCON Banner Marking When There Are NOFORN Portions	98
57. Example of NOFORN Marking.....	98
58. Example of NOFORN Markings with REL TO Portions.....	99
59. Example of PROPIN Marking.....	100
60. Example of RELIDO Marking.....	101
61. Example of FISA Marking.....	102
62. Example of EXDIS Marking	103
63. Example of NODIS Marking.....	104

64. Example of SBU Marking104
65. Example of SBU-NF Marking105

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5143.01, “Under Secretary of Defense for Intelligence (USD(I)),” October 24, 2014, as amended
- (b) DoD Instruction 5200.01, “DoD Information Security Program and Protection of Sensitive Compartmented Information,” October 9, 2008, as amended
- (c) DoD 5200.1-R, “Information Security Program,” January 14, 1997 (cancelled by Volume 1 of this Manual)
- (d) Executive Order 13526, “Classified National Security Information,” December 29, 2009
- (e) Executive Order 13556, “Controlled Unclassified Information,” November 4, 2010
- (f) Parts 2001 and 2002 of title 32, Code of Federal Regulations
- (g) DoD 5200.1-PH, “DoD Guide to Marking Classified Documents,” April 1997 (hereby cancelled)
- (h) Directive-Type Memorandum 04-009, “Security Classification Marking Instructions,” September 27, 2004 (hereby cancelled)
- (i) Directive-Type Memorandum 05-008, “Use of the ‘Not Releasable to Foreign Nationals’ (NOFORN) Caveat on Department of Defense (DoD) Information,” May 17, 2005 (hereby cancelled)
- (j) DoD Manual 5105.21, Volume 1, “Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security,” October 19, 2012
- (k) DoD Manual 5105.21, Volume 2, “Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security,” October 19, 2012
- (l) DoD Manual 5105.21, Volume 3, “Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities,” October 19, 2012
- (m) Intelligence Community Directive 710, “Classification Management and Control Markings System,” June 21, 2013
- (n) Director of National Intelligence, “Authorized Classification and Control Markings Register” (current version)¹
- (o) Director of National Intelligence, “Intelligence Community Classification and Control Markings Implementation Manual” (current version)¹
- (p) International Organization for Standardization Standard 3166-1:2006, “Codes for the Representation of Names of Countries and Their Subdivisions,” current edition²
- (q) DoD Manual 5200.45, ‘Instructions for Developing Security Classification Guides,’ April 2, 2013

¹ This document is For Official Use Only (controlled unclassified information). It is available to authorized recipients on SIPRNET (<http://www.intelink.sgov.gov/sites/ssc/capco/default.aspx>), on JWICS (<http://www.intelink.ic.gov/sites/ppr/security/ssc/capco/default.aspx>), or from the ODNI Controlled Access Program Coordination Office

² Available at <http://www.iso.org>

- (r) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
- (s) DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012
- (t) National Security Agency/Central Security Service Policy Manual 3-16, "Control of Communications Security (COMSEC) Material," August 2005
- (u) Executive Order 12951, "Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems," February 22, 1995
- (v) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
- (w) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014
- (x) National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 2, 2000³
- (y) DoD Instruction S-5105.63, "Implementation of DoD Cover and Cover Support Activities (U)," June 20, 2013
- (z) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (aa) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (ab) United States Security Authority for NATO Affairs Instruction 1-07, "Implementation of North Atlantic Treaty Organization (NATO) Security Requirements," April 5, 2007⁴
- (ac) DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)," February 27, 2006
- (ad) Committee on National Security Systems Policy 18, "National Policy on Classified Information Spillage," June 2006⁵
- (ae) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
- (af) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," February 6, 2013
- (ag) DoD Manual 5205.07, Volume 4, "Special Access Program (SAP) Security Manual: Marking," October 10, 2013
- (ah) Section 2011, et seq., of title 42, United States Code (also known as "The Atomic Energy Act of 1954, as amended")
- (ai) Subpart A of Part 1045 of title 10, Code of Federal Regulations
- (aj) DoD Instruction 5210.02, "Access to and Dissemination of Restricted Data and Formerly Restricted Data," June 3, 2011
- (ak) DoD Instruction 5210.83, "DoD Unclassified Controlled Nuclear Information (UCNI)," July 12, 2012
- (al) Section 552 of title 5, United States Code (also known as "The Freedom of Information Act")

³ Provided to designated disclosure authorities on a need-to-know basis from the Office of the Deputy Under Secretary of Defense (Policy Integration) and Chief of Staff

⁴ Available from the Central U.S. Registry

⁵ Available at <http://www.cnss.gov/Assets/pdf/CNSSP-18.pdf>

- (am) Director of Central Intelligence Directive 6/6, “Security Controls on the Dissemination of Intelligence Information,” July 11, 2001⁶
- (an) Director of National Intelligence Memorandum, E/S 00045, “Guiding Principles for Use of the ORCON Marking and for Sharing Classified National Intelligence with U.S. Entities,” March 11, 2011⁷
- (ao) Director of Central Intelligence Directive 6/7, “Intelligence Disclosure Policy,” June 30, 1998⁶
- (ap) DoD Instruction 5030.59, “National Geospatial-Intelligence Agency (NGA) LIMITED DISTRIBUTION Geospatial Intelligence (GEOINT),” March 10, 2015
- (aq) Sections 1801, et seq. of title 50, United States Code (also known as “The Foreign Intelligence Surveillance Act of 1978, as amended”)
- (ar) DoD 5400.7-R, “DoD Freedom of Information Act Program,” September 4, 1998, as amended
- (as) Executive Order 12333, “United States Intelligence Activities,” December 4, 1981, as amended
- (at) Parts 120 through 130 of title 22, Code of Federal Regulations (also known as “The International Traffic in Arms Regulations”)

⁶ SIPRNET at <https://intelshare.intelink.sgov.gov/sites/ssc/capco/capco%20web%20part%20pages/dcid-.aspx>

⁷ Classified document available to qualified recipients on a need-to-know basis from the ODNI Controlled Access Program Coordination Office

ENCLOSURE 2

OVERVIEW

1. MARKING STANDARD. This marking system augments and further defines the markings requirements established in References (d), (e), and (f), as applicable, for overall classification and portion marks.

a. The marking system specifies a uniform list of authorized security classification and control markings and their authorized abbreviations and portion markings.

b. Documents marked in accordance with previous guidance need not be re-marked with markings compliant with guidance in this Volume. All newly created documents (original and derivative) shall carry compliant markings.

c. The marking standard includes a requirement to add the applicable dissemination control markings to the overall classification line and to portion markings. Primary changes to the DoD marking system implemented by this standard are:

(1) The overall classification line is referred to as the “banner line.”

(2) The applicable dissemination control marking(s) (e.g., REL TO (authorized for release to)) shall be included in the banner line and the portion markings.

(3) The portion marks for subjects and titles shall be placed before the subject or title, as for other text. The previous exception to the placement rules for subjects and titles is no longer authorized.

(4) The standard for annotating dates in the classification authority block is YYYYMMDD. (This format is consistent with the metadata standard; see paragraph 2.h of Enclosure 3.)

(5) Markings must appear in the order specified in Enclosure 4.

(6) The format for markings will follow the syntax specified in Enclosure 4.

d. Defense Intelligence Components and personnel working with intelligence and intelligence-related information under the purview of the DNI shall refer to IC Directive (ICD) 710 (Reference (m)), the “Authorized Classification and Control Markings Register” (Reference (n)) (hereafter called the “CAPCO Register”) issued by the Office of the Director of National Intelligence (ODNI) Controlled Access Program Coordination Office (CAPCO), and the “IC Classification and Control Markings Implementation Manual” (Reference (o)) (hereafter called the “Marking Implementation Manual”) for guidance on marking and dissemination of classified and unclassified intelligence information. The CAPCO Register and Marking Implementation Manual are available electronically on the Joint Worldwide Intelligence Communications System

(JWICS) at <http://www.intelink.ic.gov/sites/ppr/security/ssc/capco/default.aspx> and on the SECRET Internet Protocol Router Network (SIPRNET) at <http://www.intelink.sgov.gov/sites/ssc/capco/default.aspx>.

2. EXAMPLES. All figures and associated markings used in this document are unclassified and are for example only. The markings used in the figures are to illustrate the required format. In order to keep this document unclassified, unclassified memorandums or other samples are used as the basis for some of the examples. The contents of the example documents are not relevant except to the extent they provide further explanation or highlight particular points.

3. WAIVERS INVOLVING MARKING OF CLASSIFIED INFORMATION. Only the Director of the Information Security Oversight Office (ISOO) may grant waivers to the marking requirements specified by References (d) and (f) for classified information. Any portion marking waiver approved will be temporary and will have specific expiration dates. Administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver. Requests for waivers from the non-Intelligence DoD Components, including those involving SAPs, should be forwarded to the Office of the Deputy Director for Intelligence (Counterintelligence, Law Enforcement, & Security) (DDI(CL&S)), for submission to the Director, ISOO. DoD Components that are elements of the IC shall furnish a copy to the DDI(CL&S), when submitting waiver requests in accordance with DNI policy. A waiver request shall include:

a. Identification of the information (or class of documents) for which the marking waiver is sought.

b. A detailed explanation of why the Director, ISOO, should grant the waiver.

c. The DoD Component's judgment of the anticipated dissemination of the information for which the waiver is sought.

d. For portion marking waiver requests:

(1) The extent to which the documents subject to the waiver may be a basis for derivative classification.

(2) How the DoD Component intends to eliminate or mitigate the negative impact that the lack of portion marking has on the sharing of information, as appropriate, between and among the DoD Components, Executive Branch agencies, and foreign partners and allies, as well as State, local, and tribal governments, law enforcement agencies, and the private sector.

(3) A statement of support from the Under Secretary of Defense for Intelligence, the Secretary of Defense's designee for security policy matters. DoD elements of the IC shall also provide a statement of support from the DNI.

e. For waiver requests involving prescribed standard forms, the proposed alternative form must be submitted with the request.

4. COVER SHEETS AND CLASSIFICATION LABELS

a. Classified files, folders, and similar groups of documents shall have clear classification markings on the outside of the folder or holder. Attaching the appropriate classified document cover sheet (Standard Form (SF) 703, “Top Secret (Cover sheet);” SF 704, “Secret (Cover sheet);” or SF 705 “Confidential (Cover sheet)”) to the front of the folder or holder shall satisfy this requirement. These cover sheets need not be attached when the item is in secure storage (e.g., GSA-approved security container).

b. If not otherwise marked, the SF classification labels listed in subparagraphs (1) through (3) of this paragraph should be used to identify the highest level of classified information stored on information technology (IT) systems and removable electronic storage media. These labels may also be used on other forms of property to clearly identify the classification level of the information contained in or on that item, when appropriate. In an environment in which both classified and unclassified information is processed or stored, SF 710, “Unclassified (Label)” shall be used to identify unclassified media or equipment. There is no requirement to use SF 710 in environments where no classified information is created or used. If the level of classification of the information on the medium changes (i.e., the information is declassified, downgraded, or upgraded), the label shall be replaced or covered by the appropriate label for the new level of classification.

(1) SF 706, “Top Secret (Label)”

(2) SF 707, “Secret (Label)”

(3) SF 708, “Confidential (Label)”

c. Where cover sheets and classification labels are used, the specified SFs must be used unless a waiver is granted in accordance with section 3 of this enclosure.

5. TRIGRAPHS AND TETRAGRAPHS. Trigraphs which are compatible with the International Organization for Standardization (ISO) Standard 3166 (ISO-3166) (Reference (p)) for country names and a partial list of approved international organization and alliance tetragraphs are available at <https://www.intelink.gov/sites/ousdi/hcis/sec/icdirect/information/default.aspx> under “Additional Resources.” Complete, current listings of approved country trigraphs and international organization and alliance tetragraphs are posted on the CAPCO websites listed in paragraph 1.d of this enclosure.

6. REQUESTS FOR OPERATIONAL TETRAGRAPHS

a. Process

(1) All requests for new tetragraphs or changes to an existing tetragraph contained in the Tetragraph Table in Annex A of the CAPCO Register, except as provided in subparagraph 6.a.(2) of this section, shall be submitted to DDI(CL&S), for review and, as appropriate, endorsement, prior to forwarding to CAPCO. Allow 90 days for processing such requests, although submission is encouraged as soon as the need is defined. All requests for action within 30 days must include justification.

(2) Requests for changes to tetragraphs that are solely changes to the existing country list shall be sent directly to CAPCO, with a copy to the DDI(CL&S). Justification or other supporting documentation must be included with such requests.

(3) Care should be taken to ensure all requests are appropriately classified.

(4) It is the requesting organization's responsibility to notify its workforce and any recipients (foreign or domestic) of the newly created or modified tetragraph, once approved.

b. Considerations. When proposing a new tetragraph, consider:

(1) Frequency of use and stability of the associated membership list. The membership list should not change frequently (i.e., not more than twice a year).

(2) Tetragraph development. The proposed tetragraph must be four alphabetic characters; the same character may not be repeated four times (e.g., RRRR). It should not spell out an actual word and may not be close to or duplicate an approved tetragraph.

(3) Significant impacts to information systems if the request is approved and/or if the membership list changes.

(4) Foreign disclosure office concerns and coordination.

c. Request Requirements. Requests for new operational tetragraphs shall include:

(1) Proposed tetragraph code and full title with classification level and foreign disclosure decision(s) associated with each, if classified. For classified tetragraphs, provide the appropriate classification authority block.

(2) List of member countries or organizations in alphabetical order, with classification level and foreign disclosure decision if classified when associated with the tetragraph code or its title.

(3) A description of the intent or purpose for the tetragraph, and the impact(s) if the marking is not approved and how that will be addressed. Attach documentation that supports the request.

(4) When the request is intended to remove a country from an existing tetragraph, a description of actions to be taken to prevent continued dissemination (including electronic dissemination) of classified information to a country that is no longer involved in the exchange and how continued protection of classified information already released will be ensured.

(5) A detailed explanation of foreign disclosure office concerns, if any. If none, so state.

(6) Requested date of incorporation into the CAPCO Register.

(7) Identification of the point of contact, giving name, title, organization, phone number and e-mail address. The point of contact will be expected to provide responses to questions and to inform the DDI(CL&S), and CAPCO of any changes in status that impact the tetragraph's listing.

ENCLOSURE 3

MARKING PRINCIPLES

1. MARKING REQUIREMENT. All classified information shall be identified clearly by marking, designation, or electronic labeling. If physical marking of the medium containing classified information is not possible, then identification must be accomplished by other means. The term “marking” includes other concepts of identifying the classification of the information. Markings, designations, and electronic labeling shall be conspicuous and immediately apparent and shall:

- a. Alert holders to the presence of classified information.
- b. Identify, as specifically as possible, the exact information needing protection and the level of protection required.
- c. Give information on the source(s) of and reasons for classification of the information.
- d. Identify the office of origin and document originator applying the classification markings.
- e. Provide guidance on information sharing, and warn holders of special access, dissemination control, or safeguarding requirements.
- f. Provide guidance on downgrading and declassification for classified information.

2. GENERAL GUIDELINES

a. The proper marking of a classified document is the specific responsibility of the original or derivative classifier (i.e., the author or originator of the information). Derivative classifiers shall refer to the source document(s), security classification guide(s), or other guidance issued by the original classification authority (OCA) when determining the markings to apply. Security Classification Guides will be developed in accordance with DoDM 5200.45 (Reference (q)), and this Manual.

b. The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the informational text and shall be conspicuous enough to alert anyone handling the document that it is classified.

c. The holder of an improperly marked classified document shall contact the document originator to obtain correct markings and shall apply those marking as required.

d. No classification or other security markings may be applied to any article or portion of an article that has appeared in a newspaper, magazine, or other public medium. If an article is

evaluated to see if it contains classified information, record the results of the review separately. However, the article and the evaluation may be filed together.

e. To facilitate information sharing and declassification processes, whenever practicable a classified attachment, addendum, annex, enclosure, or similar section shall be used when classified information constitutes only a small portion of an otherwise unclassified document. Alternately, a separate product that permits dissemination at the lowest level of classification possible or in unclassified form may be prepared.

f. If a classified document has components likely to be removed and used or maintained separately, mark each component as a separate document. Examples are annexes or appendices to plans, major parts of reports, or reference charts in a program directive. If an entire major component is unclassified, it may be marked on its face, top and bottom "UNCLASSIFIED," and a statement added: "All portions of this (annex, appendix, etc.) are Unclassified." No further markings are required on such a component.

g. Particular attention must be given to information intended for display on websites authorized to host classified information to ensure that the information carries all appropriate markings. Since web technologies permit data access without viewing the initial and/or cover pages, page and portion markings are especially important to ensure users are alerted to the presence of classified information and the level of protection it requires.

h. Metadata and/or other tags shall be applied to electronic data as required by DoDI 8320.02 (Reference (r)) and its implementing guidance. Metadata and tags shall be used to the greatest extent possible to facilitate electronic handling and dissemination of classified information.

(1) Security metadata for classified electronic information shall, to the extent possible, identify the classification level and any control and dissemination caveats required.

(2) Documents released in electronic format shall have their metadata and other electronic tags and labels reviewed for classified information prior to release. Metadata and other electronic tags and labels associated with information in electronic format shall be updated or deleted, as necessary, to reflect the actual classification and other attributes of declassified or downgraded information. Care must be taken to ensure the metadata accurately reflects the information it describes and that classified attributes are not released with unclassified data.

3. REQUIRED MARKINGS ON CLASSIFIED DOCUMENTS. All classified documents shall bear the information identified in this section; however, in exceptional cases specific information required by this section may be excluded if it reveals additional classified information. The information is to be shown using these marking elements: banner lines; portion marks; Component, office of origin, and date of origin; and classification authority block (OCA or derivative). Specific requirements for each marking element are discussed in sections 5 through 8 of this enclosure; the figures in this enclosure provide examples of correct usage. Material other than ordinary paper (and comparable electronic) documents shall have the same

information either marked on it or made immediately apparent to holders by another means. The required information is:

- a. The overall classification of the document (i.e., Confidential, Secret, or Top Secret).
- b. Identification of the specific classified information in the document and its level of classification.
- c. Component, office of origin, and date of origin.
- d. Identification of the basis for classification of the information contained in the document and of the OCA or derivative classifier.
- e. Declassification instructions and any downgrading instructions that apply.
- f. Identification of special access, dissemination control, and handling or safeguarding requirements that apply.

4. **SPECIAL NOTICES.** In addition to the information specified by section 3 of this enclosure, special notices may be required for specific types or categories of information by this Manual or other DoD issuances. Unless another directive or legal authority prescribes different placement, these notices shall be placed on the face of the document.

- a. Technical data, as specified in DoDI 5230.24 (Reference (s)), shall be marked with the distribution statements identified in section 24 of this enclosure. If determined to be export-controlled, the warning statement specified by Reference (s) shall be added.
- b. The special notice “COMSEC Material - Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance” shall be placed on the face of classified documents handled within the COMSEC Material Control System, when required by National Security Agency/Central Security Service Policy Manual 3/16 (Reference (t)). Apply it when the document is created.
- c. Other notices are identified in Enclosure 4 with the discussion of the associated marking for the specific type of information. Among the information requiring special notices are North Atlantic Treaty Organization (NATO), Restricted Data (RD), Formerly Restricted Data (FRD), Critical Nuclear Weapon Design Information (CNWDI), For Official Use Only (FOUO), CUI, and Foreign Intelligence Surveillance Act (FISA).
- d. When appropriate, classified information that is subject to specific limitations may be marked with notices such as: “Reproduction requires approval of originator or higher DoD authority.”

5. BANNER LINES

a. The banner line shall specify the highest level of classification (Confidential, Secret, or Top Secret) of information contained within the document and the most restrictive control markings applicable to the overall document (hereafter referred to as “overall classification”). See Figure 1.

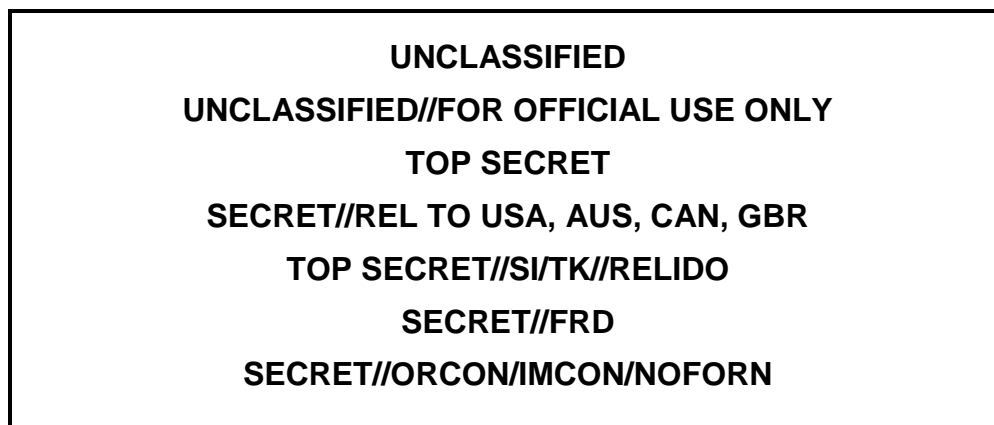
(1) The highest level of classification is determined by the highest level of any one portion within the document.

(2) The classification level in the banner line must be in English and spelled out completely. Only one classification level shall be used.

(3) Any other control markings (e.g., dissemination control markings) included may be spelled out or abbreviated as shown in this Volume.

(4) Banner line markings always use uppercase letters.

Figure 1. Examples of Banner Markings



b. Conspicuously place the banner line at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any) or last page, of each classified document. Banner line markings are usually centered on the page.

(1) The appropriate markings shall be printed, stamped, or otherwise affixed (with a sticker, tape, etc.) as specified. Material other than ordinary paper (and comparable electronic) documents must have the same information either marked on it or made immediately available to holders by another means. (See sections 16, 17, and 18 of this enclosure for additional guidance.)

(2) If the document has no front cover, the first page shall 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.

c. Each interior page of a classified document shall be marked with a banner line at the top and bottom of the page. Banner markings used on interior pages are also referred to as page markings.

(1) The banner line on an interior page shall specify either the highest level of classification of information on that page or "UNCLASSIFIED" if there is no classified information on the page, along with the applicable control markings, or alternatively, all interior pages of the document may be marked with the overall classification of the document and any applicable control markings.

(2) Use of page markings that specify the classification and control markings applicable to the information contained on that specific page requires extreme caution since:

(a) Edits or repagination may cause information of a different classification or requiring different or additional control markings to move to the page from the page before or the page after.

(b) Paragraphs may begin on one page and continue onto a second page, requiring the user to ensure that the page markings on the second page properly reflect the classification and control markings contained in the paragraph's portion markings as stated on the first page.

d. U.S. documents and other products containing foreign government information (FGI) shall carry an overall classification level of either the classification of the U.S. information or the U.S. equivalent of the FGI's classification, whichever is higher. (See section 19 of this enclosure and section 9 of Enclosure 4 of this Volume for further guidance.)

e. It is optional to mark "UNCLASSIFIED" in the banner line of hard copy documents that are unclassified and bear no control markings, except as provided in subparagraph 17.b.(7) of this enclosure.

f. Control markings are used in the banner line (and portion markings) to identify special control systems that provide additional access control or physical protection for the information or items covered by the program (e.g., SCI) or to identify the expansion or limitation on the distribution of information (i.e., dissemination controls). These markings are in addition to and separate from the level of classification.

(1) In the banner line, double forward slashes (//) separate the classification level and control markings.

(2) Multiple entries may be chosen from the control marking categories if applicable. If multiple entries are used, they are listed in the order in which they appear in Enclosure 4 and are separated by a single forward slash (/).

6. PORTION MARKS. Every classified document shall show, as clearly as is possible, which information in it is classified and at what level. Derivatively classified documents shall be portion marked in accordance with their source.

a. Every portion (e.g., subject, title, paragraphs, sections, tabs, attachments, classified signature blocks, bullets, tables and pictures) in every classified document shall be marked to show the highest level of classification that it contains. When deciding whether a subportion is to be treated as a portion and separately marked, the criterion shall be whether the marking is necessary to avoid over-classification of any of the information or to eliminate doubt about the information’s classification level. If there are different levels of classification among a portion and any of its subportions, then all subportions shall be treated as individual portions and marked separately.

b. Portion markings shall be included at the beginning of the respective portion as this position affords maximum visibility to the reader. Thus, the classification level shown always applies to the text immediately to the right of the portion marking.

c. To indicate the appropriate classification level, the symbols “(TS)” for Top Secret, “(S)” for Secret, and “(C)” for Confidential shall be used (see Figure 2). Portions which do not meet the standards for classification shall be marked with “(U)” for Unclassified.

Figure 2. Examples of Portion Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

(U)	(C)	(S)	(TS)	(U//FOUO)	(S//NF/PROPIN)
(C//FRD)	(//GBR S)	(TS//SI//TK//RELIDO)	(S//RD)		
(S//REL)	(TS//REL TO USA, AUS, CAN, GBR)	(S//RD-N)			

d. Portion marks shall include any control markings applicable to the portion (see Figure 2). Within the portion marking, double forward slashes (/) shall separate classification and control markings. Single forward slashes (/) shall separate multiple control markings within the same category (see Enclosure 4, section 1). Hyphens (-) are used to separate control markings and their sub-controls. If multiple control markings are used, they are listed in the order in which they appear in Enclosure 4.

e. Portion markings always use uppercase letters and are enclosed in parentheses.

(1) For numbered or lettered paragraphs or subparagraphs, the portion marking goes after the number or letter, and before the text.

(2) Portion markings for listings of references, enclosures, tabs, or attachments (e.g., as listed on memorandums or transmittal documents) shall be placed before the subject or title and shall indicate the classification of that subject or title, not the classification of the document. See section 15 of this enclosure for additional guidance and examples.

(3) Charts, graphs, photographs, illustrations, figures, drawings, and similar portions within classified documents must be marked to show their classification. The classification shall be based on the information contained in or revealed by the item. The portion marking shall be placed immediately preceding the chart, graph, etc., or within the item and shall be large enough to ensure viewers easily recognize it. Captions or titles of these portions must also be marked, as for text, and will indicate the classification of the caption or title, not of the portion (e.g., chart or graph) itself. The portion marking may be placed within the chart, graph, etc., and/or spelled out instead of being abbreviated when that more clearly identifies the classified status of the item. When possible, the marking should be integral to the item, so it is carried along with the item upon extraction.

(4) A classified signature block shall be portion marked to reflect the highest classification level of the information contained within the signature block itself.

f. If an exceptional situation makes individual markings of each portion clearly impracticable, a statement may be substituted describing which portions are classified and their level of classification. This statement shall identify the information as specifically as parenthetical portion marking. When classification is a result of compilation, the statement required by section 12 of this enclosure meets this requirement. A waiver is not required in these situations.

g. Each portion of an UNCLASSIFIED document that requires dissemination control shall be portion marked (e.g., (U//FOUO)) to show that it contains information requiring protection. Unclassified CUI will be marked in accordance with Volume 4 of this Manual. DoD Components that are elements of the IC shall mark those unclassified portions that do not require a dissemination control marking with the portion marking (U); other activities may, but are not required to, mark portions of unclassified documents that do not require dissemination control. However, if any portion not requiring dissemination control is marked "(U)," all portions of the document shall be marked.

h. A document not portion marked based on an ISOO-approved waiver must:

(1) Contain a warning which states that the document may NOT be used as a source for derivative classification.

(2) Be portion marked when transmitted outside the originating organization, unless the ISOO waiver approval explicitly provides otherwise.

7. DOD COMPONENT, OFFICE, AND DATE OF ORIGIN. Every classified document shall show on the first page, title page, or front cover (hereafter referred to as "the face of the document"), the originating DoD Component and office and the date of the document's origin. This information shall be clear enough to allow someone receiving the document to contact the preparing office if issues or questions about the classification arise. If not otherwise evident, the DoD Component and office of origin shall be identified and follow name and position on the "Classified By:" line.

8. CLASSIFICATION AUTHORITY BLOCK

a. General Requirements. The classification authority block shall appear on the face of each classified U.S. document, except as provided in subparagraph 8.a.(3) of this section, and shall indicate the authority for the classification determination and the duration of classification (i.e., declassification and downgrading instructions). The authority for the classification determination may be either original or derivative.

(1) The only requirement for the placement of the classification authority block is that it be on the face of the document. While placement on the bottom left of the page is most typical, whether it is placed on the right or left side or appears as one line is determined by available space. The classification authority block on electronic e-mails, messages, web pages and similar electronic material may appear as a single line of text (also see section 17).

(2) The standard format YYYYMMDD shall be used when specifying dates in the classification authority block.

(3) Include a “Declassify On:” line on the face of each classified U.S. Government document, except those containing RD or FRD. Documents containing both RD or FRD information and national security information (NSI) must include a “Declassify On:” line annotated as follows: “Not Applicable (or N/A) to RD/FRD portions” and “See source list for NSI portions.” The source list, which must be included and shall not be listed on the first page, must show the declassification instructions for each of the NSI sources. Do not mark documents containing only RD or FRD with declassification instructions.

(4) Downgrading instructions are not required for every classified document, but must be placed on the face of each document to which they apply. A downgrading instruction is used in addition to, and not as a substitute for, declassification instructions. Downgrading instructions shall not be applied to documents containing FGI, RD, or FRD.

b. Original Classification

(1) On the face of each originally classified document (see Figure 3), regardless of the media, the OCA shall apply these classification authority block markings:

(a) Classified By: List name and position title or personal identifier of the OCA. Include the DoD Component and office of origin if not otherwise evident.

(b) Reason: Cite the reason for classification.

(c) Downgrade To: If applicable, identify the lower level of classification at which the document should be safeguarded and date or independently verifiable event upon which the downgrading should take place. Note that a downgrading instruction is used in addition to, and not as a substitute for, declassification instructions.

(d) Declassify On: Specify the date or independently verifiable event for declassification or, as provided in subparagraph 8.b.(5) of this section, an approved exemption category.

(2) Identify the OCA by name and position title or personal identifier. If the information normally included on the "Classified By:" line would reveal classified information not evident from the rest of the document, complete the "Classified By:" line with an unclassified personal identifier that can be traced through secure channels.

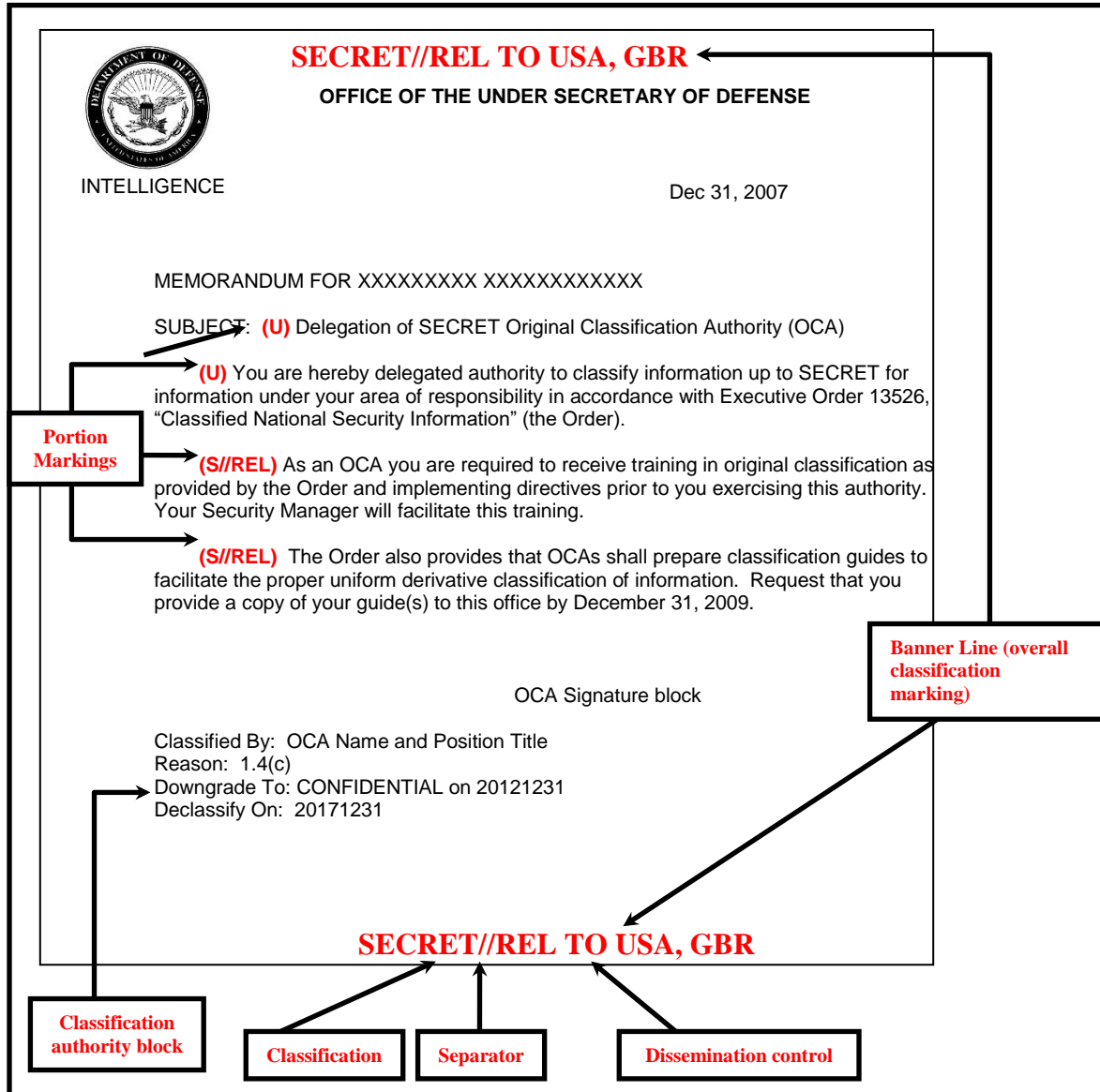
(3) If some information was originally classified at the time of preparation of the document and other information was derivatively classified, use the markings required for derivative classification. Identify the OCA by name and position title or personal identifier on the "Classified By:" line. Place "Multiple Sources" on the "Derived From:" line and maintain a record of the sources on or with the document. As part of that record, cite as one of the sources "Originally Classified Information" and identify the OCA and provide all information required for an original classification decision (i.e., provide the full classification authority block for the originally classified information).

(4) Identify the reason for classification by citation of the number "1.4" plus the letter(s) that corresponds to the appropriate category of information listed in section 1.4 of Reference (d). The OCA shall additionally provide a more detailed explanation of the reason for classification when that is not apparent from the content of the information (e.g., when classified by compilation). The categories, lettered as they appear in section 1.4 of Reference (d), are:

- (a) Military plans, weapons systems, or operations.
- (b) Foreign government information.
- (c) Intelligence activities (including covert action), intelligence sources or methods, or cryptology.
- (d) Foreign relations or foreign activities of the United States, including confidential sources.
- (e) Scientific, technological, or economic matters relating to the national security.
- (f) U.S. Government programs for safeguarding nuclear materials or facilities.
- (g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.
- (h) The development, production, or use of weapons of mass destruction.

Figure 3. Example of Originally Classified Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



(5) The OCA should select, to the greatest extent possible, the declassification instruction that will result in the shortest duration of classification.

(a) The declassification instruction shall specify:

1. A date or independently verifiable event less than 10 years from the date of the original classification;

2. A date 10 years from the date of the original classification;

3. A date or independently verifiable event greater than 10 and less than 25 years from the date of the original classification;

4. A date 25 years from the date of the original classification;

5. “50X1-HUM” for information that is clearly and demonstrably expected to reveal the identity of a confidential human source or a human intelligence source (do not include a declassification date or event); or

6. “50X2-WMD” for information that is clearly and demonstrably expected to reveal key design concepts of weapons of mass destruction (do not include a declassification date or event).

7. “25X” with date or event, designating a duration of up to 50 years from the date of original classification,* when classifying information that clearly falls within an exemption from automatic declassification at 25 years that has previously been approved by the ISCAP.

(b) For originally classified documents, the date of the original classification decision is the date of the document.

(c) The “Declassify On:” line for originally classified information may specify an exemption category (e.g., 25X1 through 25X9), with date or event, only when the originally classified information clearly falls under a pre-existing Interagency Security Classification Appeals Panel (ISCAP) approved exemption. See Volume 1, Enclosure 5, sections 13 through 15, of this Manual for additional information on exemptions. Include, following identification of the exemption category, the specific ISCAP-approved date or event for declassification.

c. Derivative Classification

(1) The face of each derivatively classified document shall include a classification authority block consisting of these elements (see Figure 4): “Classified By,” “Derived From,” and “Declassify On.” Declassification and downgrading instructions, which may be added to the

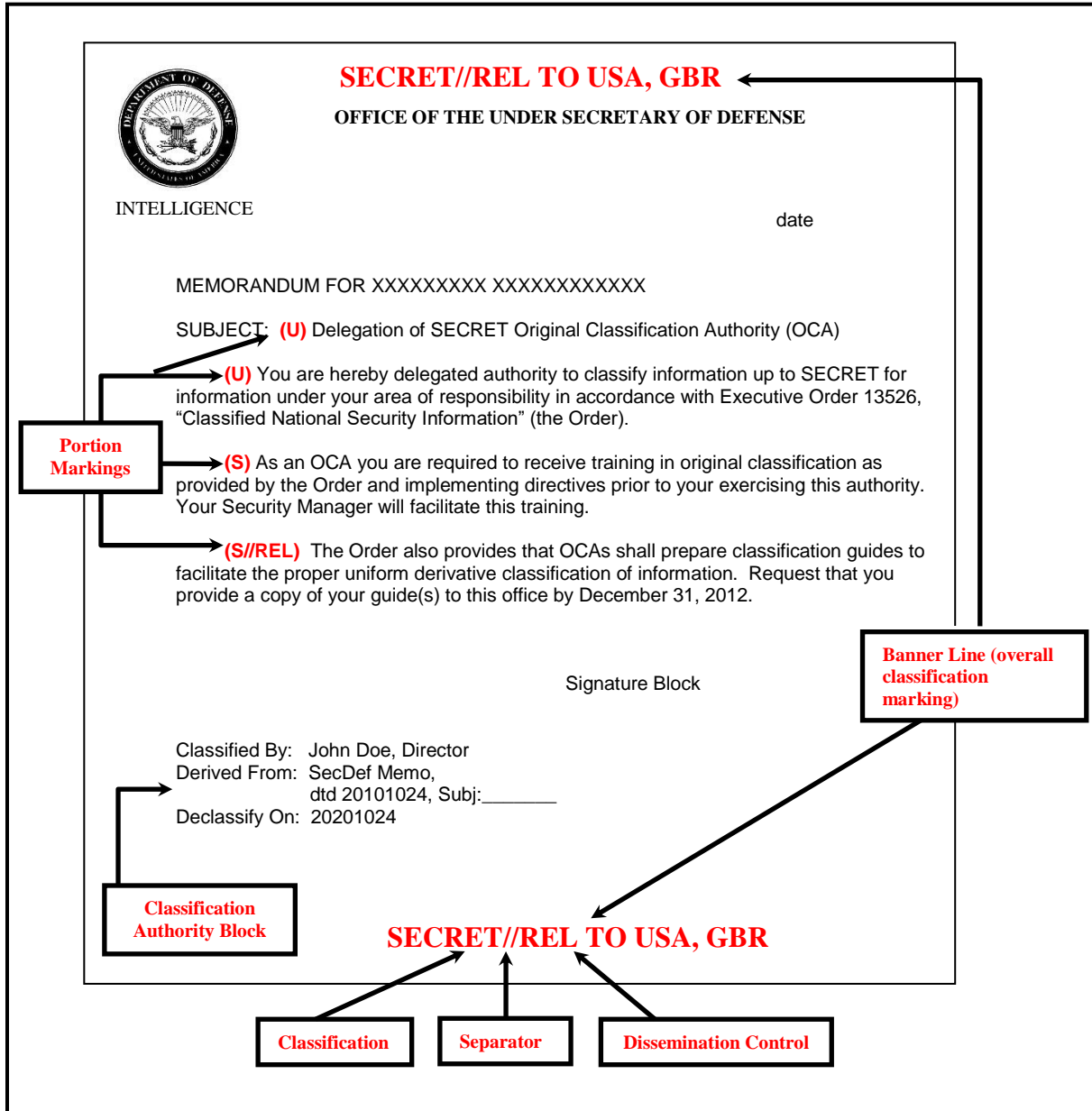
classification authority block when applicable, shall be carried forward by the derivative classifier from the source document(s), from instructions in the appropriate security classification guide(s), or from other classification guidance issued by the OCA.

(a) Classified By: List name and position title or personal identifier of the DERIVATIVE classifier and, if not otherwise evident, include the Component and office of origin.

(b) Derived From: Concisely cite the source document or classification guide used for the classification determination, to include the originating Component or agency and, where available, office of origin; type of document (e.g., memorandum, security classification guide, or message); subject; and date. Do not carry forward information from the “Derived From” line on the source document; cite the source document itself (i.e., the document from which the information is obtained or extracted).

Figure 4. Example of Derivatively Classified Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



(c) Downgrade To: If applicable, identify the lower level of classification at which the document should be safeguarded and date or event upon which the downgrading should take place. Note that a downgrading instruction is used in addition to, and not as a substitute for, declassification instructions.

(d) Declassify On: Specify the date or event for declassification, exemption category with date or event for declassification, or other declassification instruction corresponding to the longest period of classification among the source document(s), security classification guide(s), and other applicable classification guidance issued by the OCA.

(2) When multiple sources (i.e., more than one security classification guide, source document, or combination of these) are used to produce a derivatively classified document:

(a) The “Derived From:” line shall state “Multiple Sources.”

(b) The list of multiple sources shall be included with or annotated on the derivative document. If the document has a bibliography or reference list, this may be used as the list of sources. Annotate it to distinguish the sources of classification from other references.

(3) When a document is derivatively classified on the basis of a single source document that is itself marked “Derived From: Multiple Sources,” the “Derived From:” line shall cite the specific source document, not “Multiple Sources.”

(4) If a security classification guide is used to determine the declassification date of a derivatively classified document, use the declassification instructions provided by the OCA. A date derived or calculated in accordance with instructions in the guide shall not exceed 25 years from the date of the creation of the derivative document, except for information that would reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, or for which the guide cites an authorized exemption category. For example, if the guide specifies duration of “25 years,” the declassification date is 25 years from the date of the creation of the derivative document.

(5) If all the information in the document has the SAME declassification instruction assigned, place that instruction on the “Declassify On:” line. The allowable options are a date for declassification, an event for declassification, an exemption marking with associated date or event for declassification, or the markings “50X1-HUM” or “50X2-WMD.”

(6) If the document is classified by “multiple sources” and different declassification instructions apply to information included, determine the MOST RESTRICTIVE declassification instruction that applies to any of the source information (i.e., the one farthest in the future giving the longest period for classification) and place it on the “Declassify On:” line. This will ensure all of the information in the document is protected for as long as necessary. The guidance in the subparagraphs below typically provides the most restrictive date and the longest period for classification, but in some specific cases (e.g., for some 25X instructions) the hierarchy specified may not provide the correct results. In ALL cases, one must determine the period of classification for each source document and select the MOST RESTRICTIVE declassification instruction to carry forward.

(a) When determining the most restrictive declassification instruction, this hierarchy applies:

1. An ISCAP approved 75-year exemption (i.e., 75X1 through 75X9) with date or event for declassification.

2. 50X1-HUM or 50X2-WMD.

3. An ISCAP approved 50-year exemption (i.e., 50X1 through 50X9) with date or event for declassification.

4. An ISCAP approved 25-year exemption (i.e., 25X1 through 25X9) with a date or event for declassification.

5. A specific date or event for declassification, within 25 years of the creation of the derivative document.

6. Absent a declassification instruction or other declassification guidance from the OCA, a calculated date 25 years from the date of the creation of the derivative document in accordance with subparagraph 8.c.(7) of this section.

(b) If declassification dates are specified for all of the source documents, place the LATEST date (i.e., the date farthest in the future) on the “Declassify On:” line. (Example: If the information is extracted from documents marked for declassification on 20110320 (i.e., March 20, 2011), 20120601 (i.e., June 1, 2012) and 20150403 (i.e., April 3, 2015), use “Declassify On: 20150403.”)

(c) If the sources of classification indicate a combination of date(s) and event(s), indicate that declassification should occur on the latest date or the occurrence of the event(s), whichever is later. (Example: One source specifies “Declassify On: 20140803”; the other is marked “Declassify On: Completion of tests.” Mark the derivatively classified document “Declassify On: 20140803 or Completion of tests, whichever is later.”)

(d) When necessary, use the date or event for declassification associated with a 25, 50, or 75-year exemption to determine which marking is the most restrictive. Where an exemption marking is determined to be the most restrictive, also carry forward the associated date or event for declassification.

(7) If a document does not specify a definitive date or event for declassification or an exemption category, determine its declassification date in accordance with this subparagraph and use that date when determining the most restrictive declassification instruction. Carry forward the calculated date to the “Declassify On:” line when it is determined to be the most restrictive.

(a) If the source document, classification guide, or other guidance from the OCA does not specify a declassification instruction, use a date of 25 years from the date of the creation of the derivative document.

(b) If the source document is missing both a declassification instruction and the date of its origin and there is no other guidance from the OCA, use a date of 25 years from the creation of the derivative document.

(8) Follow the guidance in section 9 of this enclosure, when the source document or classification guide contains any of these declassification instructions: “Originating Agency’s Determination Required,” “OADR,” “Source marked OADR,” “Manual Review,” “MR,” Source

marked MR,” “DCI Only,” “DNI Only,” or any of the markings “X1,” “X2,” “X3,” “X4,” “X5,” “X6,” “X7,” or “X8,” or “Source marked X1” or any of the other markings “X2” through “X8.” This also applies when these declassification instructions are used with “Source Marked:” and “Date of Source: [date].”


(9) Carry over the declassification instruction “50X1-human” from the source document to the derivative document.

d. Examples. Figures 5 through 7 provide examples of the required markings on various types of documents.

Figure 5. Markings on a Memorandum

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET
OFFICE OF THE UNDER SECRETARY OF DEFENSE



INTELLIGENCE date

MEMORANDUM FOR XXXXXXXXXXX XXXXXXXXXXXXXXX

SUBJECT: **(U)** Request for Data Concerning DoD Declassification Efforts

(U) The Public Interest Declassification Board (PIDB), in response to a request from the Special Assistant to the President for National Security Affairs, is considering the establishment of a National Declassification Center to ensure more efficient, consistent, and timely declassification of records of permanent historical value. To begin this process, the PIDB requests the following information:

(U) The total overall cost to comply with the automatic and systematic declassification requirements of Executive Order 13526, “Classified National Security Information,” during fiscal year 2011; and

(S//REL TO USA, CAN, GBR) The full-time equivalent number (government and contractor) engaged in such activity during the same period of time.

Signature Block

Classification markings indicate classification of title or subject, not the classification of the document.

Attachments:

- Tab A: **(U)** Tasking Memorandum
- Tab B: **(U)** Comments **(Document is classified SECRET)**

Optional

Classified By: John Doe, Director
Derived From: USD(I) Memorandum, dtd 20100205, same subject
Declassify On: 20200205

SECRET

NOTE: Since not all portions are releasable, the REL TO marking does not appear in the banner line.

Figure 6. Markings on an Action Memorandum

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

<p style="text-align: center;">SECRET</p> <p style="text-align: right;">date</p> <p>TO: USD(I)</p> <p>FROM: <i>DDI(CL&S)</i></p> <p>SUBJECT: (U) Request for Data Concerning DoD Declassification Efforts</p> <p>(U) PURPOSE: This is an example of the portion marking for a main paragraph.</p> <p>(U) COORDINATION: None</p> <p>(U) BACKGROUND:</p> <ul style="list-style-type: none">• (S) This is the portion marking for a classified primary bullet statement.<ul style="list-style-type: none">○ (U) This demonstrates that sub-bullets must also contain portion markings.• (C) This is the portion marking for a classified primary bullet statement. <p>(U) RECOMMENDATION: Sign the Memorandum at right.</p> <p style="text-align: center;">Signature Block</p> <p>Classified By: John Smith, DUSD(I&S)-DDI (CL&S) Derived From: USD(I) Memorandum, dtd 20110205, same subject Declassify On: 20210205</p> <p style="text-align: center;">SECRET</p>

Figure 7. Markings on a Staff Summary Sheet

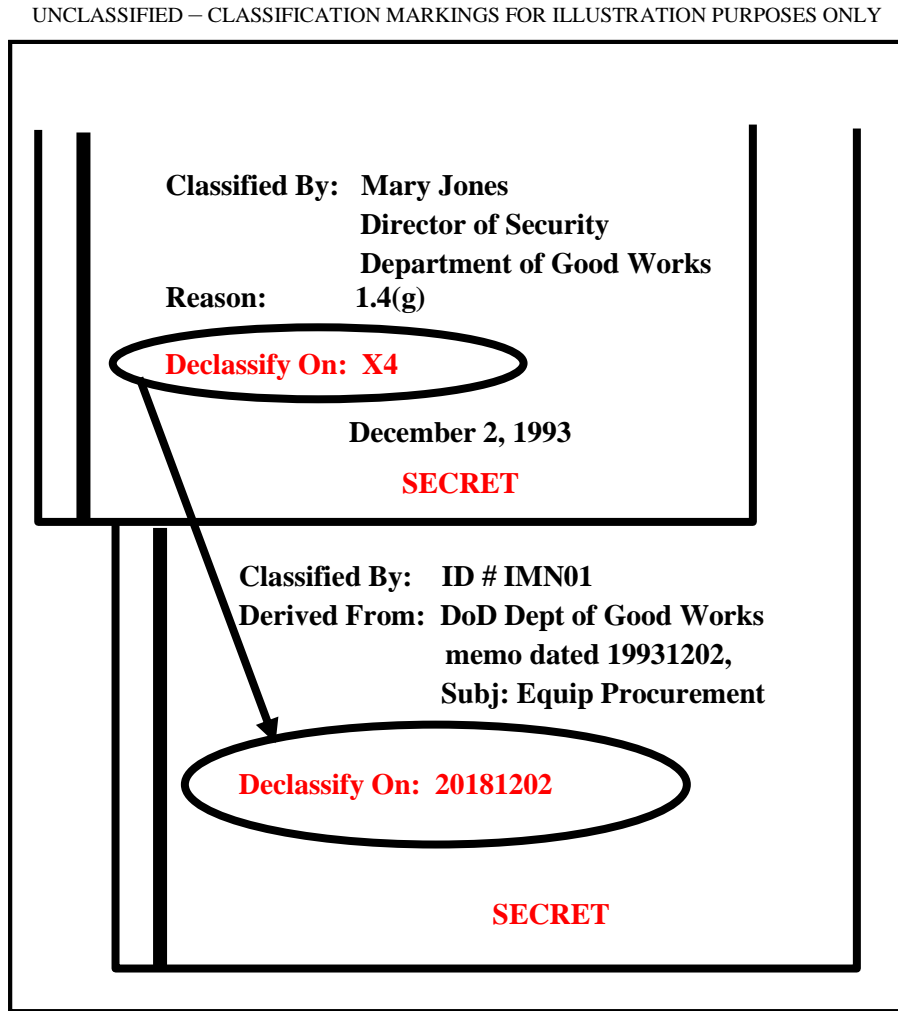
UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

TOP SECRET//NOFORN						
Tracking #	TO	ACTION	SIGNATURE (Surname) AND DATE		TO	ACTION
1	DUSD (I&S)	Coord		6		
2	PDUSD (I)	Approve		7		
3	USD(I)	Sign		8		
4				9		
5				10		
SURNAME OF ACTION OFFICER			SYMBOL/MAIL STOP	PHONE 703-604-2766	TYPIST'S INITIALS	SUSPENSE DATE
Ushman			CG2, 502C	SECURE N/A FAX N/A	PSU	
SUBJECT (U) Example of a Classified Staff Summary Sheet						DATE
						12/11/2010
<p>SUMMARY</p> <p>1. (U) Purpose.</p> <ul style="list-style-type: none"> • (TS) Show the different ways a staff summary sheet may be marked. <p>2. (U) Background.</p> <ul style="list-style-type: none"> • (TS) Point A. • (S//NF) Point B. <ul style="list-style-type: none"> ○ (S//NF) Subpoint 1. ○ (S) Subpoint 2. ○ (U) Subpoint 3. <p>3. (TS) Recommendation. Sign memorandum at right.</p> <p style="text-align: center;">Signature Block</p> <p>Attachments:</p> <p>Tab A – (U) Unclassified Title (Contents are SECRET)</p> <p>Tab B – (S) Classified Title</p> <p>CLASSIFIED BY: Name, OUSD(I) Director of Security DERIVED FROM: Appropriate SCG, Subj: XXX, dated 20090101 DECLASSIFY ON: 20201211</p> <p style="text-align: center;">TOP SECRET//NOFORN</p>						
<p>Example shows markings for paragraphs and subparagraphs, including those beginning with bullets.</p> <p>The banner line shows the highest classification in the document (TOP SECRET) and also includes the dissemination control marking NOFORN, as it is included among the portion markings for specific information.</p>						

9. USE OF CALCULATED DECLASSIFICATION DATE IN PLACE OF PREVIOUS DECLASSIFICATION INSTRUCTIONS

a. Except as provided in paragraph 9.c. of this section, when a source document is marked with any of the previously used declassification instructions listed in subparagraphs 9.a.(1) through 9.a.(5) of this section, the derivative markings shall use a calculated declassification date that is 25 years from the date of the creation of the derivative document (see Figure 8), unless other guidance from the OCA is available.

Figure 8. Use of Calculated Declassification Date



(1) “Originating Agency’s Determination Required” or “OADR” or “Source marked OADR.”

(2) “Manual Review” or “MR” or “Source marked MR.”

(3) “DCI Only.”

(4) “DNI Only.”

(5) “X1,” “X2,” “X3,” “X4,” “X5,” “X6,” “X7,” or “X8” or “Source marked X1” or any other markings “X2” through “X8.”

b. The “Derived From:” line or, if multiple sources are used, the listing of source documents shall identify the date of the source document(s), as required by subparagraph 8.c.(1)(b) of this enclosure.

c. If imagery subject to E.O. 12951 (Reference (u)) is marked with the declassification instruction “DCI Only” or “DNI Only,” use “25X1, E.O. 12951” as the declassification instruction. (Contact the National Geospatial-Intelligence Agency Classification Management Office (NGA/SISCC) for assistance in determining whether specific imagery is subject to E.O. 12951.)

d. If a security classification guide calls for the use of any of the listed declassification instructions, the procedure in paragraph 9.a. of this section shall be followed. Additionally, the holder of the classification guide should request updated guidance from the OCA, as all classification guides should reflect the requirements of References (d) and (f) and those that do not must be updated immediately.

e. When using multiple sources of information all of whose declassification dates must be calculated, the “Declassify On:” line shall be calculated using the source with the MOST RECENT DATE. (Example: In the case of three source documents, one marked “OADR” and dated September 2, 1990, one marked “MR” and dated December 3, 1992, and one marked “X3” and dated October 15, 1995, the most recent date is October 15, 1995. Mark the derivative document “Declassify On: 20201015.”)

10. MARKINGS FOR CHANGES IN CLASSIFICATION

a. Confirmation of Change. 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 for the information has not extended the classification period. This can be done by reference to a security classification or declassification guide or by consultation with the OCA.

b. Declassification. See section 11 of this enclosure for guidance on marking declassified information. Volume 1, Enclosure 5 provides additional guidance on declassification of information.

c. Downgrading. Cancel (i.e., line through) old classification markings and substitute the new ones when a document is downgraded according to its markings. For bulky documents, where changing all old markings is not practical, as a minimum, the markings on the cover (if one exists), title page (if one exists), and the first page shall be changed.

d. Downgrading or Declassification Earlier Than Scheduled. If a document is downgraded or declassified earlier than indicated by its markings, the guidance in paragraph 10.c or section 11, as appropriate, of this enclosure shall be followed. In addition, place this information on the document:

(1) The date of the downgrading or declassification re-marking.

(2) 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.

e. Upgrading. If a document is upgraded, all classification markings affected by the upgrading shall be changed to the new markings. Also, place 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).

f. 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.

g. Reclassification. Previously declassified information may be reclassified only in compliance with the requirements of paragraph 16.b of Enclosure 4 of Volume 1 of this Manual. 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.

h. 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.

11. DECLASSIFICATION MARKINGS

a. Once the holder has confirmed that the OCA for the information has not extended the classification period, information may be declassified according to markings on the document or material.

(1) The standard markings specified in paragraph 11.b of this enclosure shall be applied to declassified information, regardless of media, in accordance with section 1.6(h) of Reference (d) and section 2001.25 of Reference (f). The marking of declassified information shall not deviate from the prescribed formats unless a waiver has been approved by ISOO. Such requests shall be submitted through DDI (CL&S), in accordance with Enclosure 2, section 3.

(2) If declassification markings cannot be affixed to specific information or materials (e.g., information in some IT systems, special media, or microfilm), the originator shall provide holders or recipients of the information with written declassification instructions.

(3) Markings shall be uniformly and conspicuously applied or attached to leave no doubt about the declassified status of the information and who authorized the declassification.

b. When re-marking a document that has been declassified (see Figure 9), make sure these markings are applied:

(1) The word, "Declassified."

(2) The name and position title, or personal identifier, of the declassification authority or title and date of the declassification guide. If the identity of the declassification authority is classified, a personal identifier may be used.

(3) The date of declassification.

(4) The overall classification markings that appear on the cover page or first page are lined through with an "X" or straight line.

c. Page and portion markings on the document should also be canceled and, where practical, portion marks replaced with "(U)." Lining through the markings is sufficient to meet this requirement. For a bulky document, where canceling each page and/or portion marking is not practical, cancel, at a minimum, the markings on the front and back cover (if they exist), title page (if one exists), and the first page.

d. Declassified information shall not be released to the public until a review as required by DoDD 5230.09 (Reference (v)) and DoDI 5230.29 (Reference (w)) has been conducted to determine if there are other reasons preventing the release of the information. Regardless of the date specified for declassification, declassified information shall not be approved for public release without referral to the OCA of the information, except records accessioned by the National Archives and Records Administration (NARA) that were reviewed for automatic declassification in accordance with section 3.3 of Reference (d). Those records will be reviewed by NARA for public release.

Figure 9. Declassification Markings

DECLASSIFIED ~~SECRET~~ Unclassified

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

November 1, 2002

MEMORANDUM FOR THE DIRECTOR
From: David Smith, Chief Division 5
Subject: (U) Funding Problems

1. (U) This is paragraph 1 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

2. (S) This is paragraph 2 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses.

3. (C) This is paragraph 3 and contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses.

Declassified by: David Smith, Chief Division 5, Dept. of Good Works
Declassified on: December 31, 2019

Declassify on: December 31, 2019

David Smith, Chief Division 5
Department of Good Works
Office of Administration
1.4(a) and (d)

DECLASSIFIED ~~SECRET~~ Unclassified

Mark document as DECLASSIFIED.

Cross out old markings and replace with new markings.

Annotate authority and date of declassification

NOTE: The following cannot be declassified without a manual review by personnel appropriately certified and trained for E.O. 12958, as amended, Sec 3.3 declassification, and referral to the appropriate agency:
Restricted Data/Formerly Restricted Data, Foreign Government

12. CLASSIFICATION AS A RESULT OF COMPILATION. Classification as a result of compilation occurs when unclassified elements of information are combined and the compilation reveals classified information, or when classified elements are combined and the compilation

reveals information at a higher classification level than the individual elements. See Figure 10 for an example of marking information classified as a result of compilation.

a. Mark each portion with the classification appropriate for the information contained within the portion.

b. The banner marking for the document and all pages shall be the overall classification of the compilation. The overall classification shall be marked conspicuously at the top and bottom of each page and on the outside of the front and back covers.

c. An explanation for the classification as a result of compilation shall be provided on the "Classified By:" or "Derived From:" line or within the document. The explanation must clearly describe the circumstances under which the individual portions constitute a classified compilation, and when they do not. The explanation shall be portion marked as needed. Where specific classification guidance is provided (instead of citing the document providing the guidance), it is to be protected, using the appropriate classification or CUI marking.

13. WORKING PAPERS

a. Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers are marked in the same manner as a finished document at the same classification level when released by the originator outside the originating activity, retained more than 180 days from date of origin (30 days for SAPs), or filed permanently.

b. Working papers shall be marked as shown in Figure 11.

c. E-mail, blog and wiki entries, bulletin board posting, and other electronic messages transmitted within or external to the originating activity shall be marked as required for finished documents, not as working papers (see section 17 of this enclosure).

14. REFERENCES. When marking references and other similar lists (e.g., list of enclosures or attachments), the portion markings precede the title and indicate classification of the title, not the classification of the document. If the author wants to annotate the classification of the referenced document, a note may be included after the title as shown in Figure 12.

Figure 10. Classification as a Result of Compilation

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

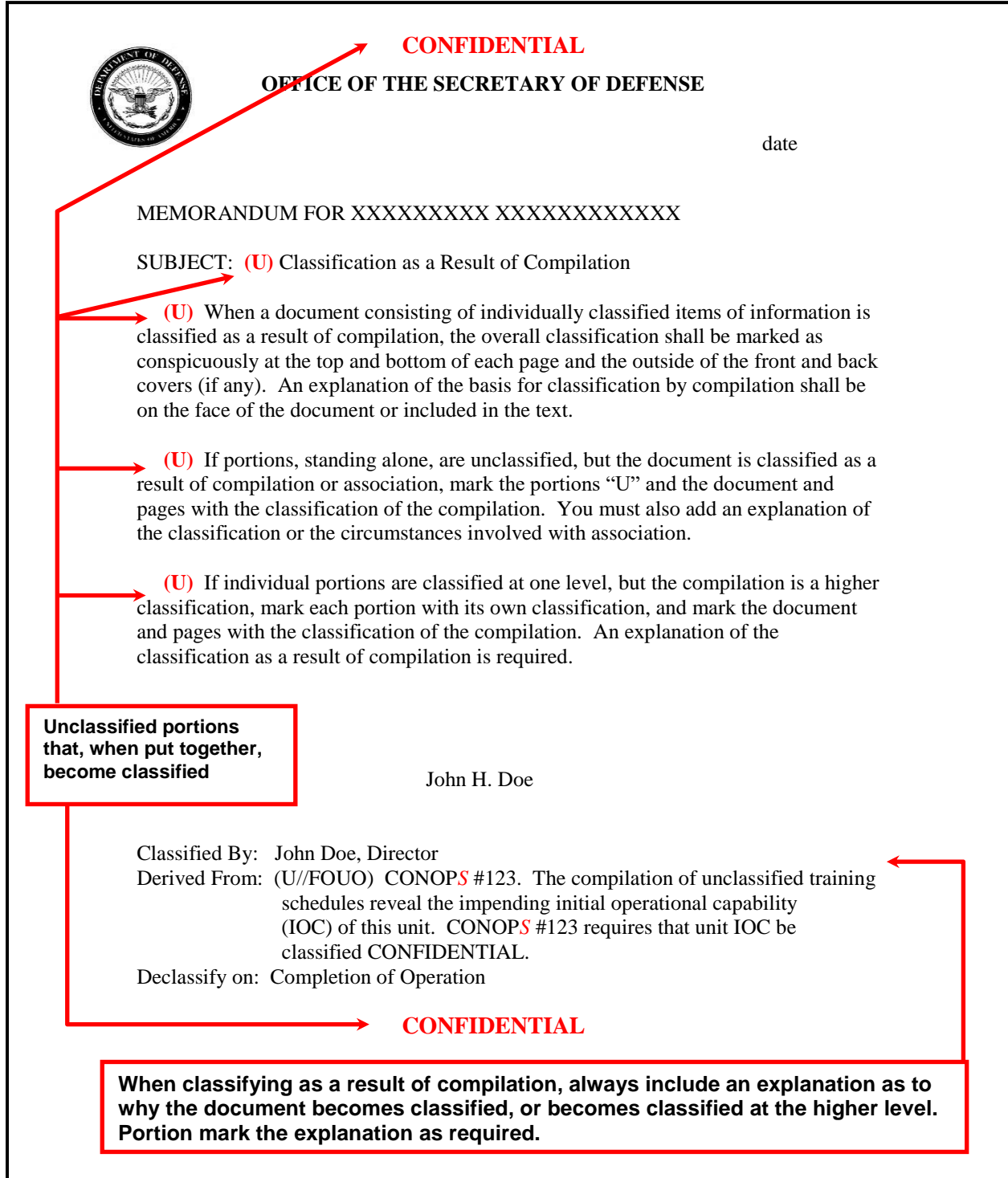


Figure 11. Markings on Working Papers

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Working papers containing classified information shall be:

- **Marked with the highest classification of any information contained in the document**
- **Dated when created**
- **Annotated "WORKING PAPER"**

• **Destroyed when no longer needed or re-marked, within 180 days, as a finished document**

Figure 12. Marking References

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

- (U) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (U) Under Secretary of Defense for Intelligence (USD(I)) Memorandum, "Security Classification Marking Instructions," September 27, 2004 (Document is classified Secret.)

15. TRANSMITTAL DOCUMENTS. Transmittal documents are documents that have information enclosed with or attached to them. An example is a letter, memo, or staff summary sheet with classified enclosures. The transmittal document itself may or may not contain classified information.

a. If the transmittal document does not contain classified information, mark the banner line with the highest classification level of any information transmitted by it. Also mark the transmittal document with an appropriate instruction indicating that it is unclassified when

separated from the classified enclosures (e.g., “UNCLASSIFIED when separated from classified enclosures” or “UNCLASSIFIED when Attachment 2 is removed”), as shown in Figure 13.

(1) If any dissemination control markings apply to the transmittal document or any enclosure, include them on the banner line of the transmittal document.

(2) Unclassified transmittal documents do not require portion marking or a classification authority block.

(3) It is not necessary to use a banner line on interior pages of an unclassified transmittal document.

(4) If any special notice (e.g., NATO, RD, FRD, or export control) applies to the transmittal document or the enclosure(s), include a statement on the face of the transmittal document highlighting inclusion of the information. Unless directed otherwise by applicable policy or regulation, a statement similar to “Document transmitted herewith contains [level of classification] RESTRICTED DATA” or “This document contains NATO [level of classification] information” will suffice.

(5) All of the marking required by section 3 of this enclosure, including classification authority block, shall appear on the classified enclosure(s) or attachment(s).

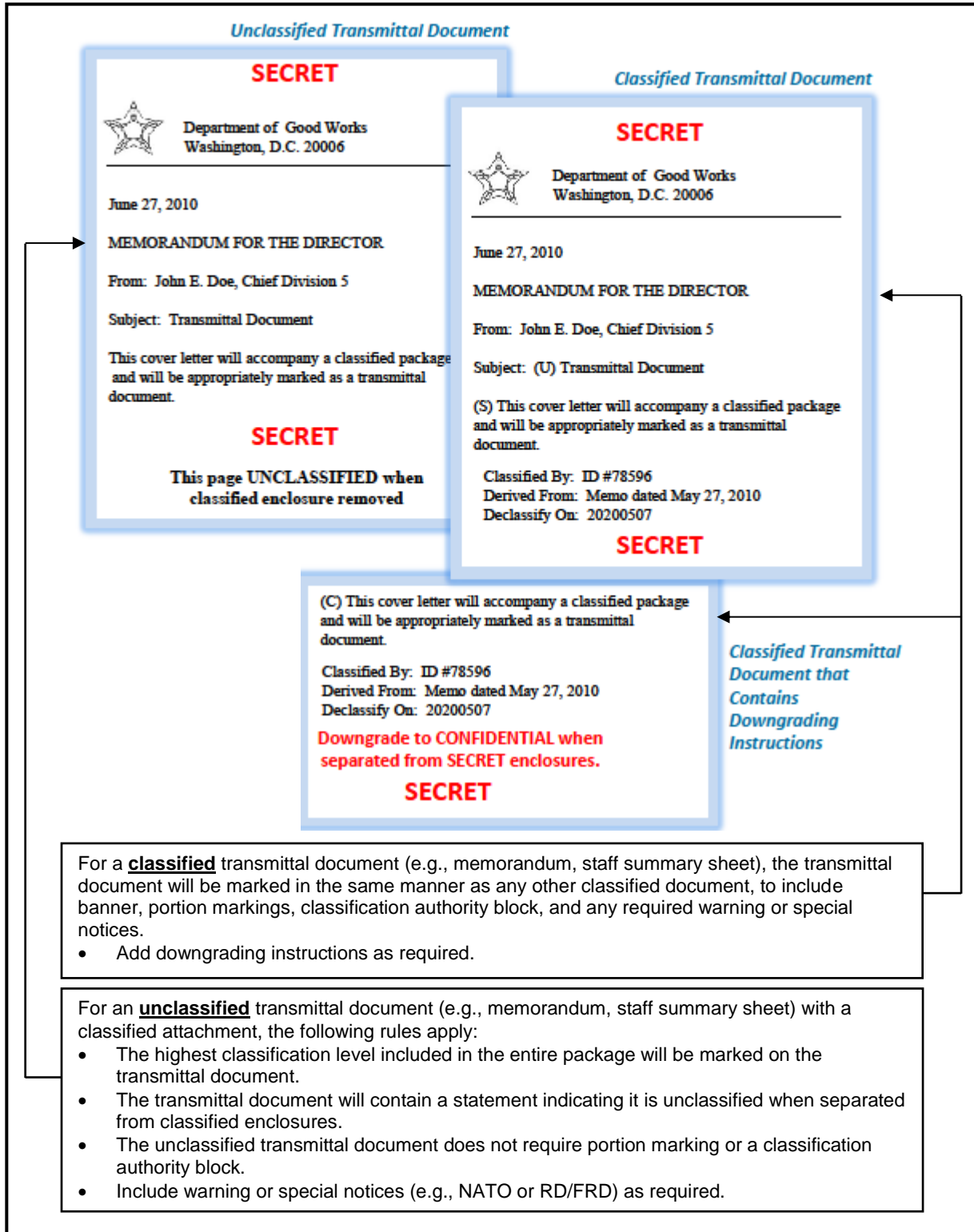
b. If the transmittal document itself contains classified information, mark it as required for all other classified information, including portion markings, classification authority block, and the full text of any applicable special notices, except:

(1) Mark the banner line of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures.

(2) Mark the transmittal document with an appropriate instruction indicating its overall classification level if the level will change when the enclosures are removed (e.g., “Downgrade to CONFIDENTIAL when separated from Secret enclosures”).

Figure 13. Transmittal Documents

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



16. **BRIEFING SLIDES.** All slides in classified briefings shall be marked as required for text documents (see Figures 14 and 15).

a. The first slide shall contain the overall classification of the presentation. The remaining slides shall be marked either with the overall classification or with the classification of the individual slide. The marking shall be large enough to ensure viewers easily recognize it.

b. The classification authority block shall be placed on the first or, less preferred, last slide. It is required only once.

c. When content of briefing slides is derived from “Multiple Sources,” place the list of sources on the first or last slide. See Figure 15 for an example.

d. All content of briefing slides, including bullets, captions, titles, and embedded graphs, charts and figures, shall be portion marked. Both classified and unclassified portions must be marked. Consistent portion marking will allow portions to be removed and placed in other documents without the danger of losing the classification level assigned to that portion. When marking charts, graphics or figures, the marking shall indicate the classification of the portion (e.g., bullet, caption, or title), not of the chart itself.

e. Hidden slides and speaker’s notes included as part of electronic briefings must be evaluated when making the overall classification determination. Hidden slides and speaker’s notes shall be marked to reflect the classification of each portion and highest classification of each slide or page in the same manner as other parts of the presentation. Unclassified briefing slides may have classified speaker’s notes which are not apparent in the typical display modes. Thus it is imperative that one always check for and evaluate any notes or hidden slides to ensure the proper classification is applied to each slide and to the briefing as a whole. Downgrading instructions such as “Downgrade to Unclassified upon removal of speaker’s notes” may be used as appropriate.

f. On complex slides where portion marking everything would be difficult and would detract from the information on the slide, use the following guidelines:

(1) When all portions are classified at the same level, mark only the overall classification on the slide. This indicates that everything on the slide is classified at that level.

(2) When a majority of the portions are classified, mark the overall classification of the slide, indicate the classification of the majority of the portions (e.g., “All portions are classified SECRET unless otherwise marked.”), and portion mark the exceptions.

(3) When a majority of the portions are unclassified, mark the overall classification of the slide, indicate that the majority of the portions are unclassified (e.g., All portions are UNCLASSIFIED unless otherwise marked.”), and portion mark the classified portions.

Figure 14. Markings on Briefing Slides

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

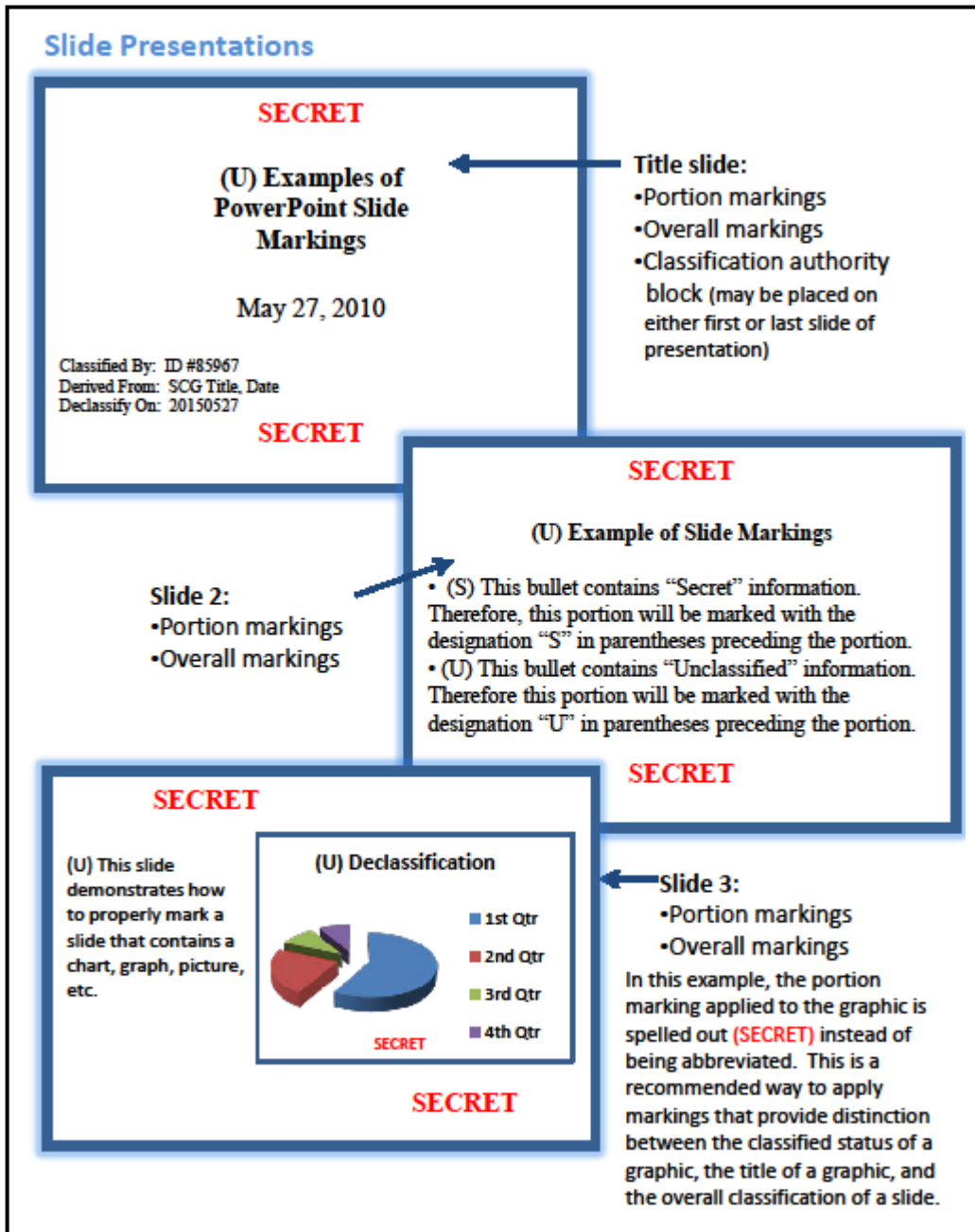
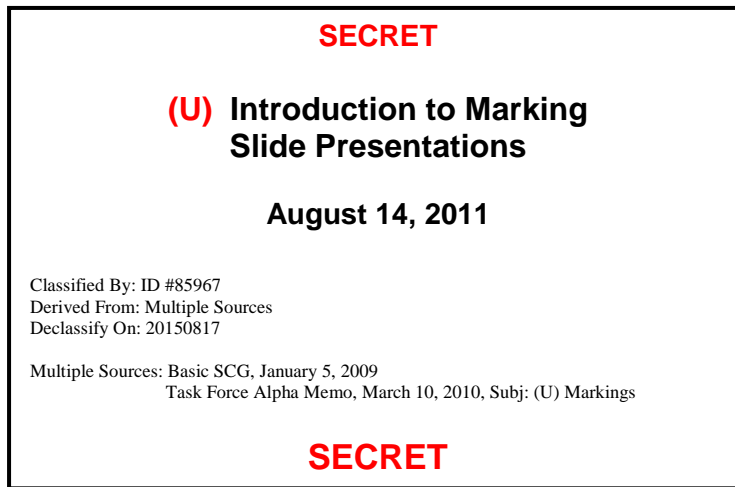


Figure 15. Multiple Source Listing on Briefing Slides

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



17. MARKING IN THE ELECTRONIC ENVIRONMENT

a. General Guidance. Where special provisions for marking some types of classified 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.

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

(a) 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.

(b) 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.

(c) 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.

(d) Prohibited for 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 (f) and this Volume.

(2) 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.

(3) 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.

(4) 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.

b. E-Mail Messages

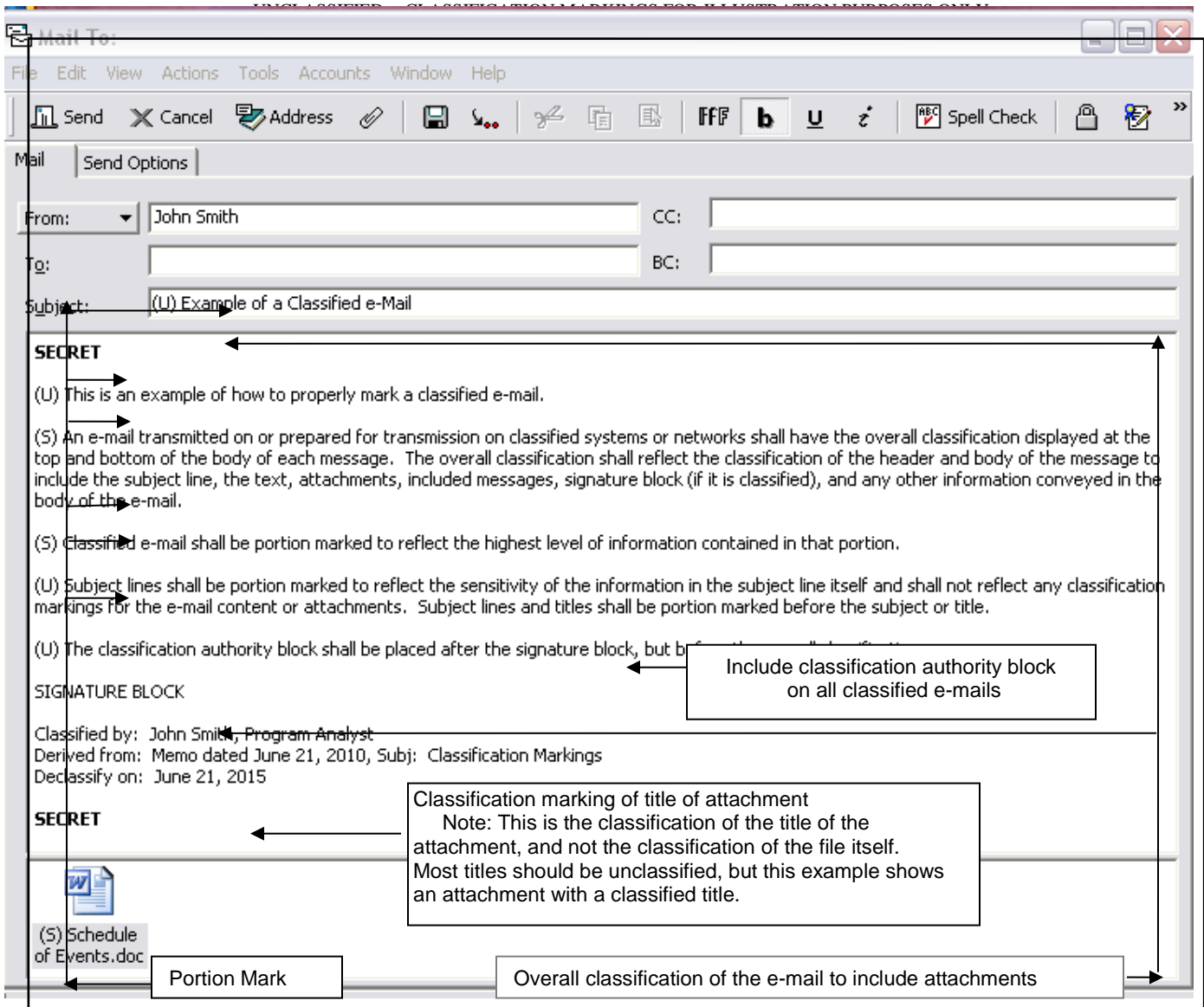
(1) E-mail transmitted on or prepared for transmission on classified systems or networks shall display the banner line at the top and bottom of the body of each message. A single linear text string showing the overall classification, to include dissemination and control markings, shall be included as 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 shall 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 shall be portion marked before the subject or title.

Figure 16. Marking E-Mails



(5) The classification authority block shall be placed after the signature block, but before the banner line at the bottom 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 shall be included.

(8) E-mails used as transmittal documents shall be marked as required by section 15 of this enclosure. Place the instruction indicating the e-mail’s overall classification level when separated from its enclosures just above the banner line at the bottom of the message.

c. Web Pages

(1) Web pages shall be classified and marked based on their own content regardless of the classification of the pages to which they link. Information to which the web page links shall also be marked based on its own content.

(2) The banner marking for a web page shall reflect the overall classification markings and any dissemination control or handling markings for the information on that page. Linear text appearing on both the top and bottom of the page is acceptable.

(3) If any graphical representation (e.g., picture, chart, diagram or other graphic) is utilized, a text equivalent of the overall classification marking string shall be included in the hypertext statement and page metadata. This will enable users without graphic display to be aware of the classification level of the page and allows for the use of text translators.

(4) Classified web pages shall be portion marked. Each portion shall be marked to reflect the highest level of information contained in that portion. A portion containing a URL or reference to another document shall be portion marked based on the classification of the content of the URL itself, even if the content to which it points requires a higher classification marking.

(5) Classified web pages shall include a classification authority block which may be placed at either the top or bottom of the page. The classification authority block may appear as single linear text string instead of the traditional appearance of three lines of text.

(6) Electronic media files such as video, audio, images, or slides shall carry the overall classification and classification authority block, unless the addition of such information would render them inoperable. In such cases, another procedure or method shall be used to ensure recipients are aware of the classification status of the information and the declassification instructions.

d. URLs. URLs provide unique electronic addresses for web content and shall be portion marked, as appropriate, based on the classification of the content of the URL itself. The URL shall NOT be portion marked to reflect the classification of the content to which it points. URLs shall be developed at an unclassified level whenever possible. When a URL is classified, a portion mark shall be used in the text of the URL string in a way that does not make the URL inoperable to identify the URL as a classified portion in any textual references to that URL (see Figure 17). Additionally, any textual portion in which the URL is embedded must also be appropriately portion marked (see Figure 18).

Figure 17. Examples of URL with Included Portion Mark

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

http://www.center.xyz/SECRET/filename_(S).html
http://www.center.xyz/filename2_(TS).html
http://www.center.xyz/filename_(TS//NF).html

Figure 18. Example of Portion-Marked URL Embedded in Text

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

(TS) Further information on this project may be obtained at [http://www.organization.mil/projectname_\(TS\).html](http://www.organization.mil/projectname_(TS).html) which is available to registered users.

e. Dynamic Documents

(1) A dynamic document or page contains electronic information derived from a changeable source or ad hoc query, such as a relational database. The classification, and therefore the classification markings, for the information returned may vary depending upon the specific request.

(2) If there is a mechanism for determining the actual classification markings for dynamic documents, the appropriate classification markings shall be applied to and displayed on the document.

(3) If such a mechanism does not exist, the highest classification level of information within the data source (e.g., database) shall be used and a warning shall be applied at the top of each page of the document. Such content shall NOT be used as a basis for derivative classification. An example of such a warning is shown in Figure 19.

(a) The warning is to alert users that there may be elements of information that may be either unclassified or classified at a lower level than the highest possible classification of the information returned.

(b) Users should consult classification guide(s) and/or the data source owner (i.e., the organization with primary responsibility for the content of the database or other data source) or the specified point of contact for the classification of individual elements in order to avoid unnecessary or over-classification and/or other impediments to information sharing.

(c) The data source owner shall ensure classification guidance and points of contact are available to assist users with these inquiries.

Figure 19. Warning Statement for Dynamic Documents

This content is classified at the [insert highest classification level of the source data] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to [cite specific reference, where possible, or state “the applicable classification guide(s)”]. [Add a point of contact when needed.]

(4) Users developing a document based on or incorporating query results from a database must properly mark the document in accordance with the requirements of this enclosure. If there is doubt about the correct markings, users should contact the data source owner for guidance.

f. Bulletin Board Postings and Blogs

(1) A blog, an abbreviation of the term “web log,” is a website consisting of a series of entries, often commentary, description of events, or other material such as graphics or video, created by the same individual as in a journal or by many individuals. While the content of the overall blog is dynamic, individual entries are generally static in nature.

(2) The overall classification marking for every bulletin board or blog shall reflect the overall classification for the highest level of information allowed in that space. Linear text appearing on both the top and bottom of the page is acceptable. Individual postings or entries shall be additionally marked as required in subparagraph 17.f.(4) of this section.

(3) Subject lines of bulletin board postings, blog entries, or comments shall be portion marked to reflect the sensitivity of the information in the subject line itself, not the content of the post.

(4) Each individual bulletin board posting, blog entry, comment, or similar item shall have its own banner line reflecting the overall classification, including dissemination controls, of the subject line of the posting, the text of the posting, and any other information in the posting. The banner line shall be entered, manually or utilizing an electronic classification tool, in the first line of text and at the end of the body of the posting. These markings may appear as a single line of linear text.

(5) Bulletin board postings, blog entries, comments, or similar items shall be portion marked. Each portion shall be marked to reflect the level of information contained in that portion.

g. Wikis. A wiki is a web site that allows users to make changes, contributions, or corrections. Wikis may be classified or unclassified; users must be careful not to post classified information on unclassified sites.

(1) Initial submissions to classified wikis shall include the overall classification marking, portion marking, and the classification authority block in the same manner as described in paragraph 17.f. of this section for bulletin boards and blogs. All of these may appear as single line text.

(2) When users modify existing entries which alter the classification level of the content or add new content, they shall change the required markings to reflect the classification markings for the resulting information. The IT system shall provide a means to log the identity of each user, the changes made, and the date and time of each change to a classified wiki.

(3) Wiki articles and entries on classified wikis shall be portion marked. Each portion shall be marked to reflect the level of information contained in that portion.

h. Instant Messaging, Chat, and Chat Rooms

(1) Instant messages and chat conversations generally consist of brief textual messages but may also include URLs, images, or graphics. Chat discussions captured for retention or printing shall be marked at the top and bottom of each page with the overall classification reflecting all of the information within the discussion and, for classified discussions, portion markings and the classification authority block shall also appear.

(2) Chat rooms shall display system-high overall classification markings (i.e., the highest level of classification allowed to be on the system in accordance with the accreditation of the system being used) and shall contain instructions informing users that the information may not be used as a source for derivative classification unless it is portion marked, contains an overall classification marking, and a classification authority block.

i. Attached Files. When files are attached to another electronic message or document the overall classification of the message or document shall account for the classification level of the attachment and the message or document shall be marked in accordance with section 15 of this enclosure.

18. SPECIAL TYPES OF MATERIALS

a. General Guidance. When classified information is contained in computer or other electronic media, audiovisual media, chart and maps, or other media (including hardware, equipment, and facilities) not commonly thought of as documents, the requirement remains to identify as clearly as possible the information that requires protection, the level of protection required and its duration. The main concern is that holders and users of the material are clearly notified of the presence of classified information. The marking required by section 3 of this enclosure shall be applied in the same fashion as for documents, to the extent feasible. If it is not feasible to mark such information, an explanatory statement shall be included on or with the information that explains exactly what information is and is not classified. Other markings normally required for classified documents (see section 3 of this enclosure) shall also be made available, either on the item or in documentation that accompanies it. When information is

expected to be rendered in multiple media or formats, consider confirming that the classification markings are readable in all expected forms (e.g., when displayed on workstations, when projected, when printed, when converted to different file types). Particular requirements and exceptions are noted in the remainder of this section.

b. Blueprints, Engineering Drawings, Charts, and Maps. Mark blueprints, engineering drawings, charts, maps, and similar items not embedded in a classified document with the appropriate overall classification and dissemination control markings. The classification marking shall be unabbreviated, conspicuous, and applied top and bottom, if possible, in such a manner as to ensure reproduction on any copies. The legend or title shall also be portion marked to show classification of the legend or title. If the blueprints, maps, and other items are large enough that they are likely to be rolled or folded, the classification markings shall be placed to be visible when the item is rolled or folded. See Figures 20 and 21 for examples.

Figure 20. Markings on Maps

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

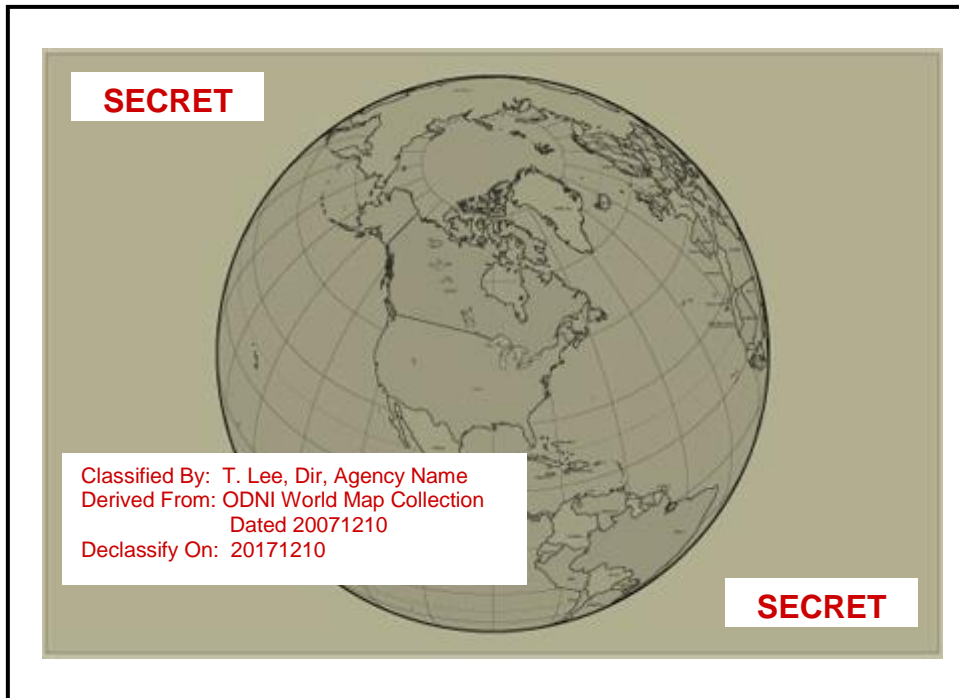
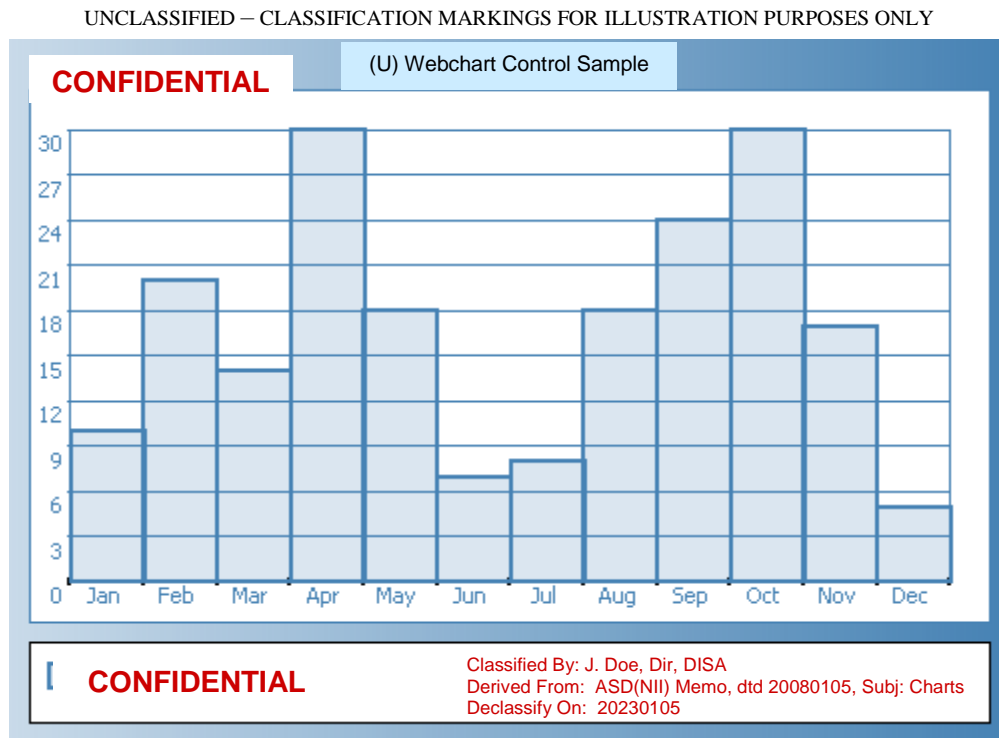


Figure 21. Markings on Charts

c. Photographic Media

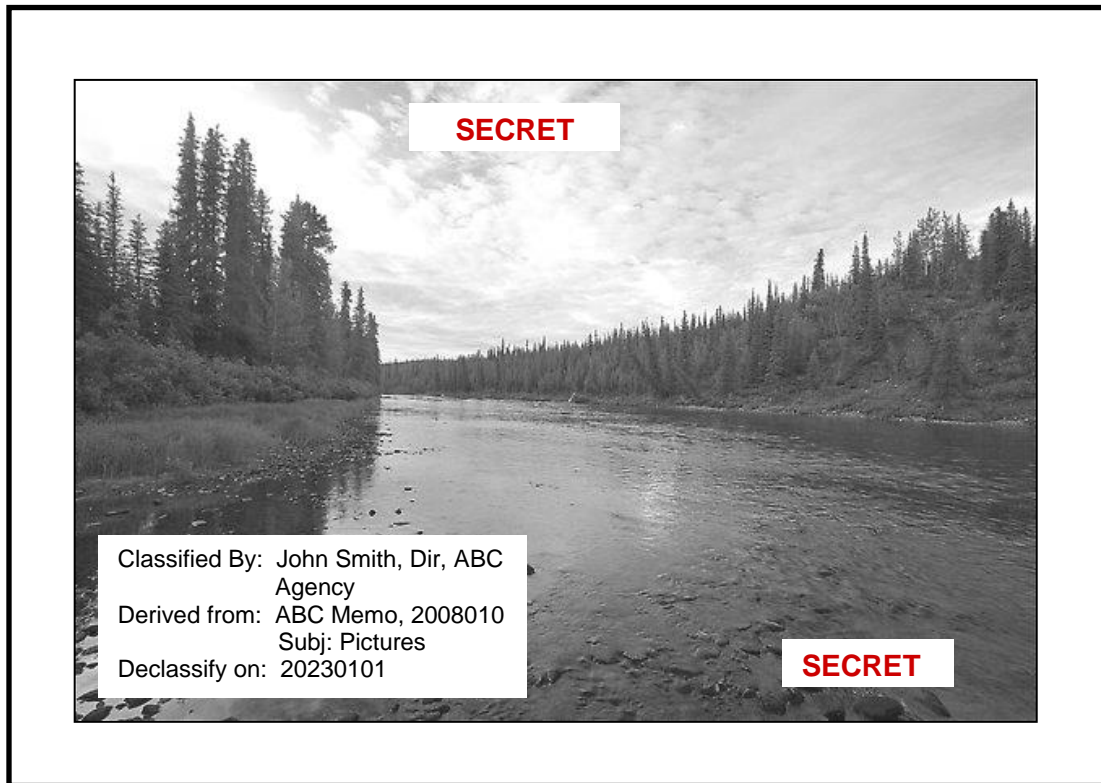
(1) Mark photographs and negatives with the overall classification and dissemination control markings applicable to information they contain (see Figure 22). Mark photographs on the face, if possible. If this cannot be done, the classification and dissemination control markings may be placed on the reverse side. Place other required markings on photographs along with the classification marking, or include them in accompanying documentation. Digital photographs may be edited to overlay markings on the face of the photograph.

(2) Mark roll negatives and positives, and other film containing classified information with their overall classification and any dissemination control markings. These markings shall be placed on the film itself, if possible, and on the canister, if one is used. If placed on the film itself, the marking shall be placed at both the beginning and end of the roll.

(3) Mark slides and transparencies with the overall classification and any control markings on the image area of the item and also on the border, holder, or frame. Place other required security markings on the first slide or transparency in a set in the image area; on the border, holder, or frame; or in documentation accompanying the item. These additional markings are not needed on the other slides or transparencies; however, slides or transparencies that are permanently removed from a set shall be marked as a separate document. Information on the image area of each slide or transparency shall be portion marked in accordance with section 6 of this enclosure.

Figure 22. Markings on Photographs

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



d. Digital Video Discs (DVDs), Video Tapes, Motion Picture Films, and Web Videos. Mark DVDs, video tapes, motion picture films, and web videos with their classification and any control markings at the beginning and end of the presentation (i.e., the played or projected portion). Other required security markings shall be placed at the beginning of the presentation. Discs, reels, and cassettes shall be marked with the overall classification of the item. When stored in a container, the container shall be marked with the overall classification, applicable dissemination control markings, and other required markings in accordance with section 3 of this enclosure.

e. Sound Recordings. Place an audible statement of overall classification and dissemination control requirements at the beginning and end of sound recordings. Reels or cassettes shall be marked with the overall classification and any required dissemination control markings and stored appropriately. When stored in a container, the container shall be marked with the overall classification, applicable dissemination control markings, and other required markings in accordance with section 3 of this enclosure.

f. Microfilm, Microfiche, and Similar Microform Media. Mark microfilm, microfiche, and similar microform media with their overall classification and applicable control markings in the

image area that can be read or copied. Such media shall have this marking applied so it is visible to the unaided eye. Other required security markings shall be placed (in accordance with section 3 of this enclosure) on the item or included in accompanying documentation. Any containers shall contain all required markings, except no markings are required if the container is transparent and markings on the media itself are clearly visible.

g. Removable Electronic Storage Media. Conspicuously mark removable storage media used with computers, IT systems, and other electronic devices (see Figure 23). (Examples of such media include, but are not limited to, compact discs, DVDs, removable hard disks, flash or “thumb” drives, magnetic tape reels, disk packs, floppy disks and diskettes, disk cartridges, optical discs, paper tape, magnetic cards, memory chips, and tape cassettes and micro-cassettes.) Internal media identification will include security markings in a form suitable for the media. All such devices bearing classified information must be conspicuously marked with the highest level of classification of information stored on the device and any dissemination control notices that apply to the information.

(1) Use SFs 706, 707, 708, or 710, as appropriate, to identify the highest level of classified information stored on IT systems and removable IT storage media, if not otherwise marked. Where size or technology preclude affixing the labels to the removable device itself (e.g., memory chips), the label may be affixed to the sleeve or container in which the device is stored. Remove SFs 706, 707, 708, or 710 labels from computers or other IT systems that use removable classified storage devices (see paragraph 18.g in this enclosure for a list of examples) when those computers or systems are no longer used to process classified media and when the computer or system does not have any residual memory or buffers that may still contain classified information.

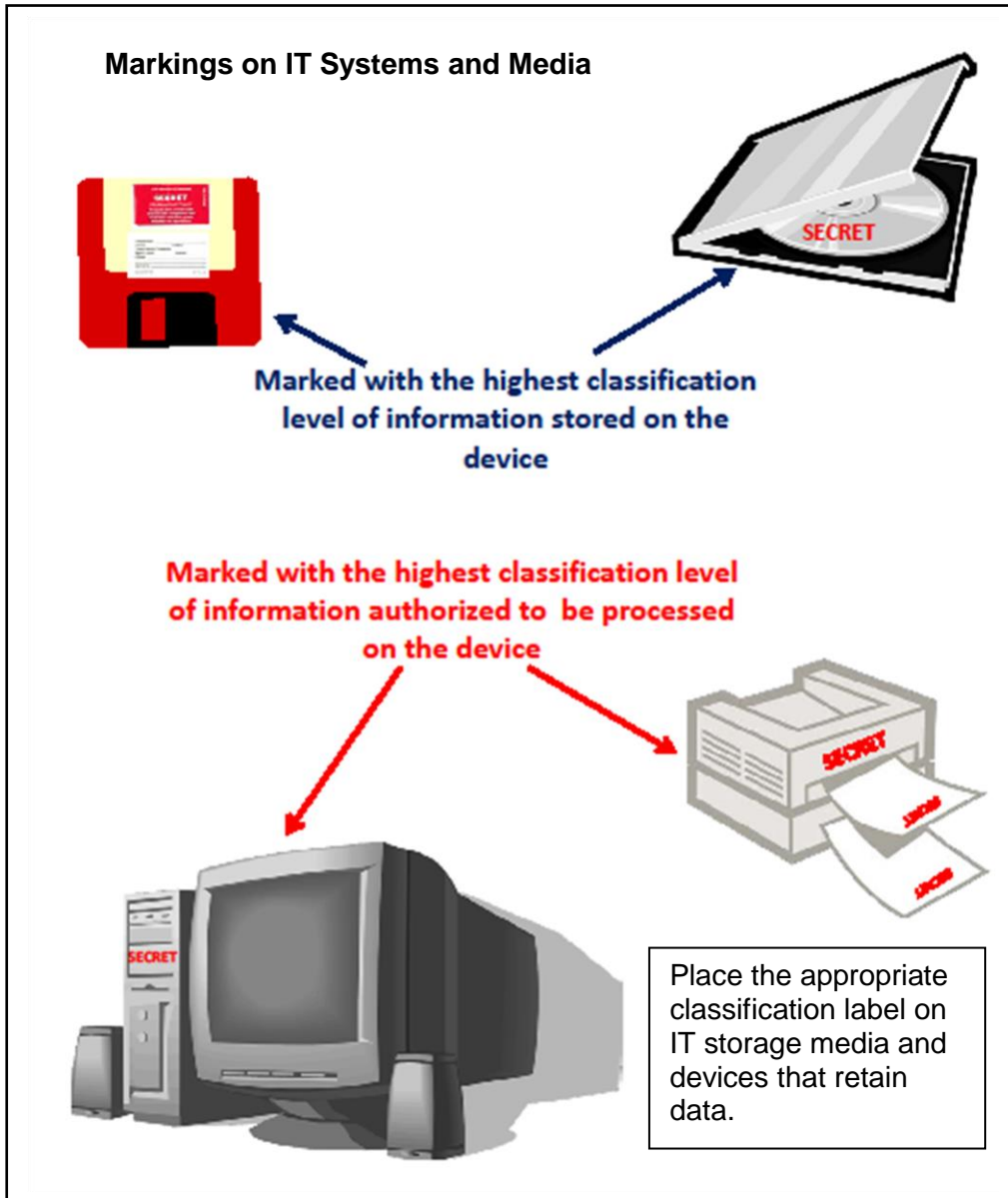
(2) Other information normally provided by document markings (e.g., classification authority block) shall be available as follows:

(a) If the required information is stored in readily accessible format on the device, it does not have to be marked on the outside of the device. As an example, if classified files or documents prepared on an IT system are stored on a DVD or compact disc, and each file bears its own declassification instructions, the disc does not need to be marked with declassification instruction. This is true with respect to most removable media containing classified text files and documents, even though a few of them may not have all of the prescribed markings.

(b) If the required information is not stored in readily accessible format on the device, it shall be marked on the outside of the device (normally with a sticker or tag) or placed on documents kept with the device.

Figure 23. Markings on IT Systems and Media

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



19. MARKING FGI

a. Most foreign governments, as well as NATO, use three classification markings that generally equate to U.S. TOP SECRET, SECRET, and CONFIDENTIAL. Many of the governments also have a fourth classification marking, RESTRICTED, for which there is no U.S. equivalent. NATO has a fifth category of controlled information, NATO UNCLASSIFIED.

Some governments also have unclassified information protected by law or national regulations that is treated, and provided to other governments, as “in confidence” information.

b. Bilateral security agreements and arrangements with other governments and NATO, as well as Reference (d), require that FGI retain its original foreign government classification markings, or be marked with a U.S. classification marking that results in a degree of protection equivalent to that provided by the foreign government or NATO markings. Therefore, if the foreign government or NATO marking is in English, and the U.S. and foreign government or NATO protective measures for the classification are equivalent, the foreign government or NATO marking may be retained on the information. However, if the FGI is marked in a language other than English, a classification marking that results in equivalent protection will be applied to the FGI.

c. Volume 3, Enclosure 2, section 17 of this Manual identifies the safeguarding requirements for FGI.

d. Section 4 of Enclosure 4 of this Volume provides specific guidance on marking documents consisting entirely of FGI; section 9 of Enclosure 4 of this Volume provides guidance on markings to be used on U.S. documents containing FGI portions; section 5 of Enclosure 4 of this Volume provides guidance on marking information that is jointly produced or owned with another country or international organization.

20. MARKING REQUIREMENTS FOR TRANSFERS OF DEFENSE ARTICLES TO AUSTRALIA OR THE UNITED KINGDOM WITHOUT AN EXPORT LICENSE OR OTHER WRITTEN AUTHORIZATION. Volume 3, Enclosure 4, section 7 of this Manual provides marking requirements for the transfer of certain classified and unclassified defense articles to Australia or the United Kingdom without an export license or other written authorization.

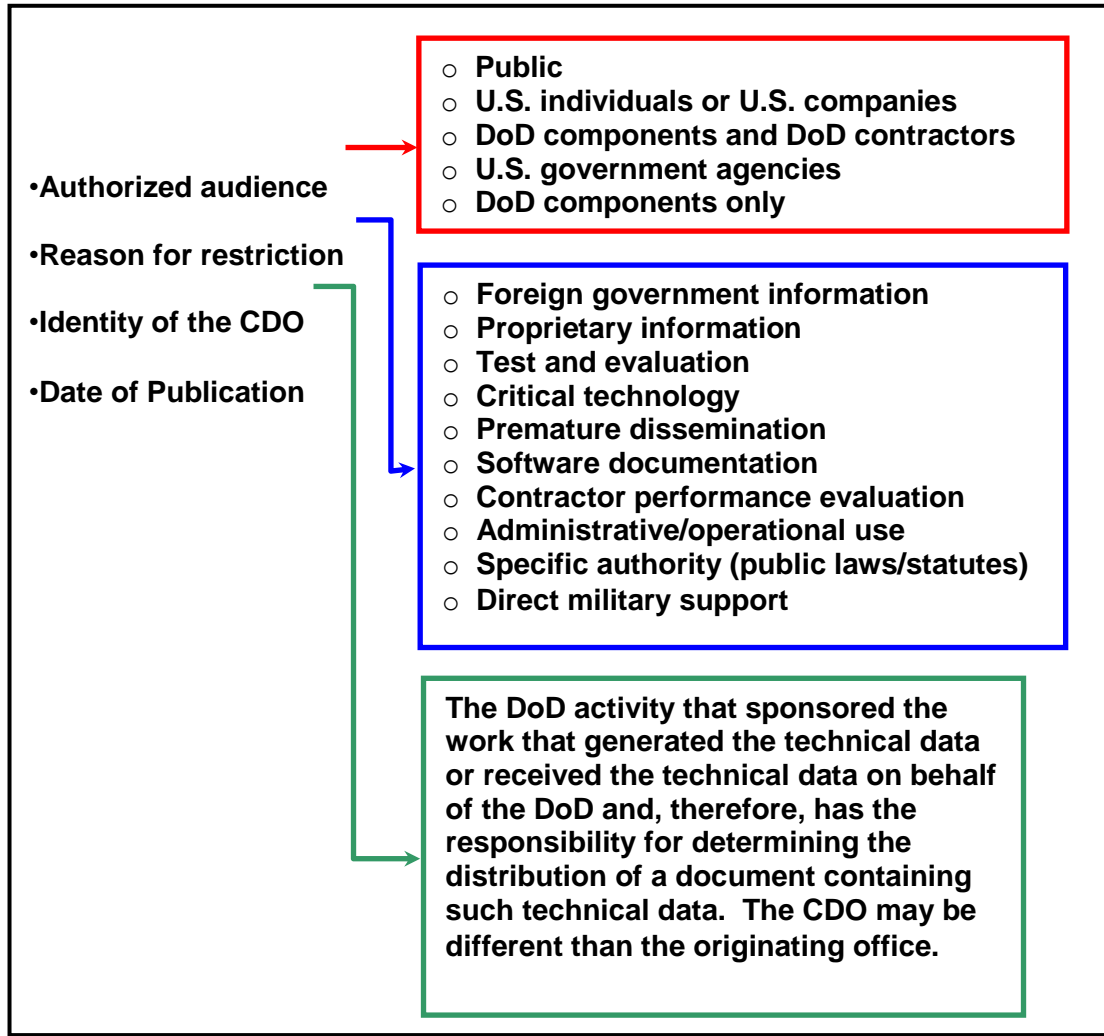
21. TRANSLATIONS. Mark translations of U.S. classified information into a foreign language with the appropriate U.S. classification markings and the foreign language equivalent. U.S. classification markings must appear as the banner line with the foreign language translation of the marking immediately below the top banner and immediately above the bottom banner within the document. The translation shall clearly show the United States as the country of origin.

22. MARKING DOCUMENTS FOR TRAINING PURPOSES OR AS AN EXAMPLE. Documents and material that contain no classified information, but which carry classification markings for training purposes or to provide an example, shall also have a marking that clearly shows the actual classification of the documents. Place a suitable marking on each page of the document or to accompany each example, such as: “Unclassified – Classification Markings for Training Purposes Only.”

23. DISTRIBUTION STATEMENTS

a. Distribution statements are used on classified and unclassified scientific and technical documents to identify the document’s availability for distribution, release, and disclosure without additional approvals and authorizations from the controlling DoD office (CDO). Each statement provides four pieces of information as illustrated in Figure 24 to facilitate secondary distribution and release.

Figure 24. Information Provided by Distribution Statements



b. All DoD Components generating or responsible for technical documents shall determine each document’s secondary distribution availability and mark it in accordance with Reference (s) before primary distribution. Authorized distribution statements are shown in Table 1. The distribution statement shall be placed conspicuously on the cover page/first page of the document.

(1) Documents recommended for public release (Distribution A) must first be reviewed in accordance with Reference (v).

(2) All security classification and declassification guides incorporating technical data shall be marked with the appropriate distribution statement.

c. All technical documents that are determined to contain export-controlled technical data shall additionally be marked with the export-control statement specified in Enclosure 4 paragraph 2.g of Reference (s).

Table 1. Authorized Distribution Statements

DISTRIBUTION STATEMENT A.	Approved for public release; distribution is unlimited.
DISTRIBUTION STATEMENT B.	Distribution authorized to U.S. Government Agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).
DISTRIBUTION STATEMENT C.	Distribution authorized to U.S. Government Agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).
DISTRIBUTION STATEMENT D.	Distribution authorized to the DoD and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).
DISTRIBUTION STATEMENT E.	Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).
DISTRIBUTION STATEMENT F.	Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD authority (applied under rare and exceptional circumstances when specific authority exists or when need-to-know must be verified).

ENCLOSURE 4

MARKING STANDARD

1. OVERVIEW. The marking standard specified by this enclosure further defines, but does not change, the markings requirements established in References (d) and (f) for overall classification and portion markings. This marking system provides specific formatting and precedence guidance to facilitate electronic processing of classified information. The hierarchy and order of markings, the specific markings that fall within each category, and the formatting structure are shown in Figure 25. Sections 2 through 11 discuss authorized markings and provide examples of usage.

a. Markings must appear in the order listed in Figure 25. This enclosure and Appendixes 2 and 3 to this enclosure discuss each marking individually.

b. The required marking syntax for classified U.S. documents is:
CLASSIFICATION//SCI//SAP//AEA//FGI//DISSEM//OTHER DISSEM.

(1) A double forward slash (//) shall be used to separate marking categories; a single forward slash (/) shall be used to separate multiple types within the same marking category, e.g., CLASSIFICATION//SCI/SCI//DISSEM/DISSEM. Hyphens (-) without interjected spaces shall be used to separate a control system from its sub-control (or compartment), e.g., SI-G or RD-N.

(2) The classification level in the banner line must be in English and spelled out completely. Other required control markings (e.g., SCI, SAP, or dissemination control markings) included in the banner line may be spelled out or abbreviated using the authorized abbreviation noted in the discussion of the specific marking.

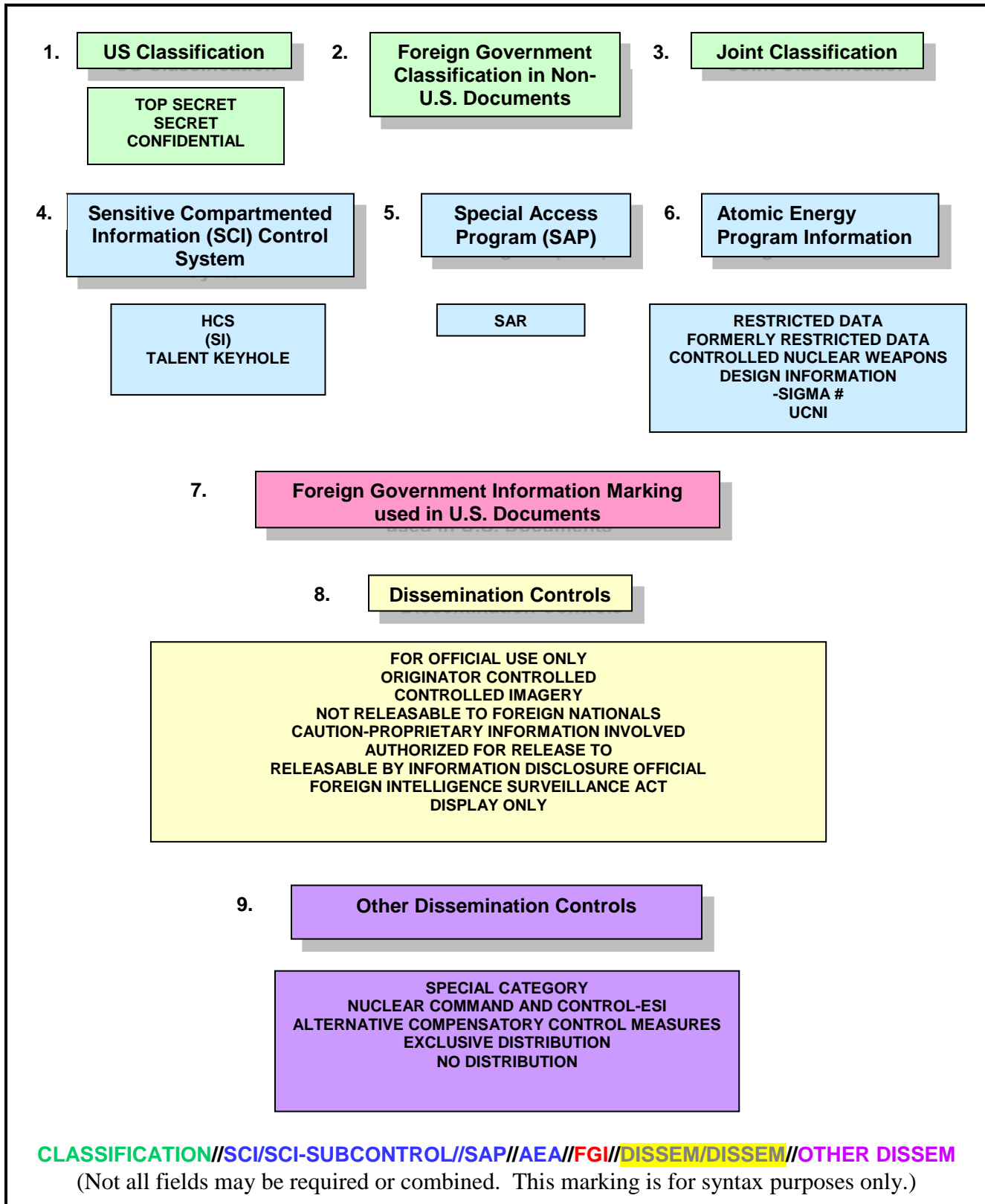
(3) Control markings (e.g., SCI, SAP, AEA, or dissemination), where applicable, are required in both the banner line and portion markings. Markings that indicate the presence of FGI or Atomic Energy Act (AEA) information are also carried in both locations. Double forward slashes (//) will separate both the classification level from the control markings, and the different categories of control markings from each other.

(4) Dissemination markings are used to identify the expansion or limitation on the distribution of information. These markings are in addition to and separate from the level of classification, and the SCI, SAP, AEA, and FGI categories.

(a) Multiple entries may be chosen from the dissemination control categories if applicable. If multiple entries are used, they are listed in the order in which they appear in Figure 25.

(b) In classified documents that contain dissemination control markings, the unclassified portions that do not require any control markings will be marked with (U).

Figure 25. Marking Structure



c. Note that the syntax for marking documents consisting solely of FGI and for jointly-produced documents is different than that for classified U.S. documents. Both begin with “//,” without a preceding classification. The syntax is:

(1) For classified non-U.S. documents: //[country code] [non-U.S. classification].

(2) For classified joint documents: //JOINT [classification] [country codes].

d. U.S. classification markings, non-U.S. classification markings, and JOINT classification markings are mutually exclusive. They may not be used at the same time in a banner line or a portion mark.

e. The term “country code” when used in the description of banner line and portion marking requirements refers to both trigraphic country codes and tetragraph codes for international organizations and coalitions.

2. USE OF THE MARKING “NOT RELEASABLE TO FOREIGN NATIONALS” (NOFORN)

a. The dissemination marking “NOFORN” is an intelligence control marking used to identify intelligence which an originator has determined meets the criteria of Reference (m) and which may not be provided in any form to foreign governments (including coalition partners), international organizations, foreign nationals, or immigrant aliens without the originator’s approval.

b. Within DoD, NOFORN is authorized for use ONLY on intelligence and intelligence-related information and products under the purview of the DNI, in accordance with DNI policy, with three exceptions. The exceptions are Naval Nuclear Propulsion Information (NNPI), the National Disclosure Policy Document (also known and hereafter referred to as “NDP-1” (Reference (x))), and cover and cover support information in accordance with DoDI S-5105.63 (Reference (y)), each of which may be marked “NOFORN.” Other than these three exceptions, there is no authorized DoD use for the NOFORN caveat on non-intelligence information. Further guidance on the proper use of the NOFORN caveat on intelligence information may be found in Appendix 2 to this enclosure.

c. DoD Components must ensure personnel are trained on proper application of the NOFORN caveat to ensure it is not applied to non-intelligence information and to facilitate intelligence sharing.

d. Although not authorized for use on DoD information, other U.S. Government uses of the NOFORN caveat exist; section 4 of Appendix 3 to this enclosure provides information on one such usage.

e. Consistent with Reference (m), NOFORN may be applied, when warranted, to unclassified intelligence information that has been determined to be properly categorized as CUI.

f. Except for the instances identified in this volume, NOFORN may not be applied to any other DoD information. Whenever such use is detected, classification challenges are encouraged in accordance with the procedures in paragraph 22, Enclosure 4, of Volume 1 of this Manual. The DoD Component's chain of command will require the proper limited use of the NOFORN dissemination control marking.

g. All existing requirements for a positive foreign disclosure decision before release to a foreign government apply, in accordance with DoDDs 5230.11 and 5230.20 (References (z) and (aa)).

3. U.S. CLASSIFICATION MARKINGS

a. Authorized U.S. classification designators are:

(1) TOP SECRET (TS)

(2) SECRET (S)

(3) CONFIDENTIAL (C)

b. U.S. classification markings are not preceded by the double slash (//) or abbreviated in the banner line (see Figure 26). (A double slash with nothing preceding it indicates that the document contains only FGI or JOINT information as described in sections 4 and 5 of this enclosure.)

Figure 26. Example of U.S. Classification Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

<p style="text-align: center;">TOP SECRET</p> <p>MEMORANDUM FOR XXXXXXXXXXXX</p> <p>SUBJECT: (U) Delegation of TOP SECRET Original Classification Authority (OCA)</p> <p>(TS) You are hereby delegated authority to classify information up to TOP SECRET for information under your area of responsibility in accordance with Executive Order 13526, "Classified National Security Information" (the Order).</p> <p>(C) As an OCA, you are required to receive training in original classification as provided by the Order and implementing directives prior to exercising this authority. Your Security Manger will facilitate this training.</p> <p>Classified By: R. Smith, Sec. of Army Derived From: Army Memorandum XYZ, dated 20071215, same subject Declassify On: 20171215</p> <p style="text-align: center;">TOP SECRET</p>

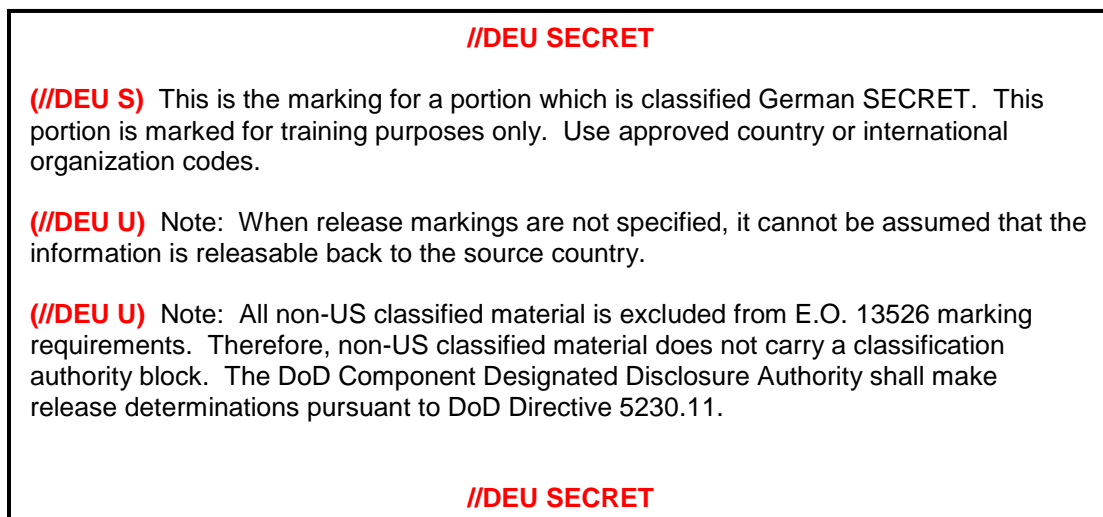
4. FGI MARKINGS USED ON NON-U.S. DOCUMENTS

a. General. This section provides guidance for marking documents consisting ENTIRELY of FGI. See section 19 of Enclosure 3 of this Volume for general guidance on marking FGI, Section 5 for marking Joint documents, and section 9 of this enclosure for markings to be used on U.S. documents containing FGI portions.

(1) All classification markings on FGI (banner and portion) shall begin with a double forward slash, “//.” The required format is: //[country code] [equivalent classification] (see Figure 27).

Figure 27. Example of Markings for Non-U.S. Documents

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



(2) The authorized equivalent classifications are:

- (a) TOP SECRET (TS)
- (b) SECRET (S)
- (c) CONFIDENTIAL (C)
- (d) RESTRICTED (R)
- (e) UNCLASSIFIED (U)

(3) Equivalent foreign government classification markings should be used in conjunction with the requirements of this section to determine the appropriate marking in subparagraph 4.a.(2). Questions regarding the equivalent foreign government markings should be directed to

the Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy.

(4) FGI classifications shall not be annotated in the banner line with U.S. classification markings or JOINT classification markings. These three marking categories are mutually exclusive in the banner lines and portion marks.

(5) No classification authority block shall be used as all non-U.S. information is excluded from the marking requirements of Reference (d).

(6) The DoD Component Designated Disclosure Authority shall make disclosure determinations pursuant to DoDD 5230.11 (Reference (aa)).

b. NATO Classification Markings. NATO information bears unique classification markings which signify that the information is protected in the NATO security system.

(1) NATO classifications are used on NATO information (i.e., information prepared by or for NATO and information of the NATO member nations that has been released into the NATO security system). Within the DoD, access to and marking and handling of NATO information is governed by USSAN Instruction 1-07 (Reference (ab)) and DoDD 5100.55 (Reference (ac)).

(2) Documents consisting entirely of NATO information shall have a banner line and portion markings consisting only of NATO markings (see Figure 28). NATO classified information does not carry a classification authority block.

(a) COSMIC is the NATO designation for TOP SECRET information whose unauthorized disclosure would cause exceptionally grave damage to NATO. Although the word "NATO" is used in the designation NATO SECRET, CONFIDENTIAL, and RESTRICTED information, the word "NATO" is never used with NATO information classified at the TOP SECRET level.

(b) The ATOMAL designation is used with U.S. RD or FRD, or UK ATOMIC information that has been officially released to NATO.

(c) The BOHEMIA designation is used for NATO TOP SECRET information that signals intelligence (SIGINT) derived and should be handled in SIGINT channels only. BOHEMIA may be used only with //COSMIC TOP SECRET.

(3) NATO banner markings may be used only on NATO information. NOFORN cannot be used on NATO information.

(4) When NATO information is incorporated into a U.S. document, the portion marking will be a NATO marking; however, the banner line will use the highest classification of information in the document (i.e., classification of the U.S. information or the U.S.-equivalent classification for the NATO information, whichever is higher) with the addition of "//FGI NATO" (e.g., SECRET//FGI NATO). The statement "THIS DOCUMENT CONTAINS NATO

(level of classification) INFORMATION” shall appear on the face of the document. See Section 9 of this enclosure for guidance on use of FGI markings in U.S. documents.

Figure 28. Examples of NATO Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

<u>NATO Banner Line</u>	<u>NATO Portion Marking</u>	
//COSMIC TOP SECRET	(//CTS)	<div style="border: 2px solid red; padding: 5px;"> <p>COSMIC is applied to TOP SECRET material that belongs to NATO. BOHEMIA is used only with NATO TOP SECRET information that is SIGINT derived.</p> </div>
//COSMIC TOP SECRET BOHEMIA	(//CTS-B)	
//NATO SECRET	(//NS)	
//NATO CONFIDENTIAL	(//NC)	
//NATO RESTRICTED	(//NR)	
//NATO UNCLASSIFIED	(//NU)	
//COSMIC TOP SECRET ATOMAL	(//CTS-A)	<div style="border: 2px solid red; padding: 5px;"> <p>ATOMAL applies to U.S. Restricted Data or Formerly Restricted Data, or UK ATOMIC information, that has been officially released to NATO</p> </div>
//SECRET ATOMAL	(//NS-A)	
//CONFIDENTIAL ATOMAL	(//NC-A)	

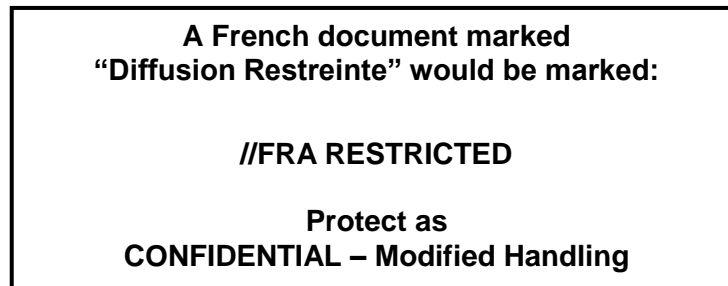
c. Documents Marked RESTRICTED or That are Provided “in Confidence.” Many foreign governments and international organizations have a fourth level of classification that generally translates as “Restricted,” and a category of unclassified information that is protected by law in the originating country and is provided on the condition that it shall be treated “in confidence.”

(1) Mark foreign government documents that have a classification designation which equates to RESTRICTED, as well as unclassified foreign government documents provided on the condition that they shall be treated “in confidence,” to identify the originating government and whether they are Restricted or provided “in confidence” (see Figure 29).

(2) Additionally, mark them “CONFIDENTIAL – Modified Handling” and protect them according to Volume 3, Enclosure 2, section 17 of this Manual.

Figure 29. CONFIDENTIAL-Modified Handling Example

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



5. JOINT CLASSIFICATION MARKINGS

a. Joint classification markings are used on information owned or produced by more than one country/international organization, or on jointly owned information developed or generated in the performance of the program to which the U.S. DoD had Joint Production /Reutilization Rights(i.e., foreground information).

b. The JOINT marking in the banner line or portion mark indicates co-ownership and implied releasability of the entire document or entire portion, as appropriate, ONLY to the originators’ respective countries, unless more restrictive controls are explicitly imposed by the originators. Further disclosure or release of JOINT information to countries other than those of the originators requires the approval of all co-owners.

c. All JOINT classification markings (banner and portion) begin with a double forward slash, “//” followed by the word JOINT (i.e., “//JOINT”)

d. The required format for classification banner markings is: //JOINT [classification] [country codes]. If the United States is NOT one of the co-owners, the classification may be RESTRICTED in accordance with authorized FGI classification markings (see paragraph 4.a.(2) of this enclosure). Where the United States is a co-owner, RESTRICTED may NOT be used.

e. Country codes, including USA, are listed in the banner line in alphabetical order followed by international organization codes in alphabetical order. This placement of “USA” is unique to the JOINT marking and should not be confused with the placement required by the REL TO marking. Codes are separated by spaces. See Figures 30 and 31 for placement examples.

Figure 30. Example of Joint Classification Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

//JOINT SECRET CAN GBR USA

(//JOINT S) This is the marking for a portion which is classified Joint Canadian, British, and U.S. SECRET. This portion is marked for training purposes only. Use ISO 3166 trigraphic country codes or registered international organization codes.

(U) The JOINT marking in the banner line indicates co-ownership and implied releasability of the entire document only to the co-owners. Further release requires approval of the co-owners.

(U) The classification authority block is required on JOINT classified information when the United States is one of the co-owners.

Classified By: Joe Doe, Dir., ABC Agency
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321215

//JOINT SECRET CAN GBR USA

Figure 31. Example of Joint Classification Marking with REL TO

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

//JOINT SECRET GBR USA//REL TO USA, AUS, CAN, GBR, NZL

(//JOINT S//REL) This is the marking for a portion which is classified Joint British and U.S. SECRET. The British and United States, as co-owners, have authorized further release to Australia, Canada and New Zealand (same as banner line). Use ISO 3166 trigraphic country codes or registered international organization codes.

(U) The JOINT marking in the banner line indicates co-ownership and implied releasability of the entire document ONLY to the co-owners. Further release requires approval of the co-owners.

(U) (REL) may be used if the portion's REL TO county list is the same as the banner line REL TO country list. When extracting a JOINT portion marked "(REL)," carry forward the country codes from the source document's banner line to the new portion mark.

Classified By: Joe Doe, Dir, ABC Agency
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20321215

//JOINT SECRET GBR USA//REL TO USA, AUS, CAN, GBR, NZL

f. Country codes are not included in the portion markings when all portions match the banner country codes. However, if a JOINT portion is extracted into a U.S.-produced non-JOINT document, then the country codes must be listed, in alphabetical order, in the portion markings (i.e., (//JOINT [classification] [country codes])).

g. When JOINT information is extracted and used in a derivative U.S. document, the JOINT portions must be segregated (i.e., must be separate portions) from U.S. classified information. The banner line of the derivative U.S. document shall show the highest classification level of all portions, expressed as a U.S. classification marking. The JOINT marking is not carried forward to the banner line, but is used in applicable portions. Additionally, FGI markings shall be added to the banner line and shall include all non-U.S. country codes identified in the JOINT portion(s). See Figure 32 for an example of this usage.

h. The classification authority block is used only when the United States is one of the co-owners.

Figure 32. Example of Joint Classification Marking in a U.S. Derivative Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//FGI GBR//REL TO USA, AUS, CAN, GBR, NZL

(//JOINT S GBR USA//REL) This is the marking for a portion which is classified JOINT British and U.S. SECRET. The British and United States, as co-owners, have authorized further release to Australia, Canada and New Zealand (same as banner line). Use ISO 3166 trigraphic country codes or registered international organization codes.

(S//REL) This portion is classified U.S. SECRET and is authorized for release to Australia, Canada, United Kingdom, and New Zealand (same as banner line).

(U) (REL) may be used if the portion's REL TO county list is the same as the banner line REL TO country list. When extracting a JOINT portion marked "(REL)," carry forward the country codes from the source document's banner line to the new portion mark.

Classified By: Joe Doe, Dir, ABC Agency
 Derived From: Memorandum XYZ, Dated 20071215
 Declassify On: 20321215

SECRET//FGI GBR//REL TO USA, AUS, CAN, GBR, NZL

6. SCI CONTROL SYSTEM MARKINGS

a. SCI is classified national intelligence information concerning, or derived from, intelligence sources, methods or analytical processes that require handling within formal access control systems established by the Director of National Intelligence (DNI). Within an SCI control system, there may be compartments and sub-compartments, which are used to further

protect and/or distinguish SCI. Users should refer to References (n) and (o) for additional guidance on SCI markings.

b. The published SCI control systems are:

- (1) HCS (HUMINT Control System).
- (2) Special Intelligence (SI).
- (3) TALENT KEYHOLE (TK).

c. Multiple SCI control system entries may be used if applicable. When multiple entries, (whether published or unpublished) are used, list them alphabetically. Use a single forward slash (/) as the separator between multiple SCI control system entries (see Figure 33). In Figure 33, “ABC” is a notional unpublished SCI control system with a notional portion marking of “ABC.” Individuals encountering information with unrecognized markings in the SCI category should contact their SSO for further guidance, as the marking may be an unpublished control system. Each example shown in Figure 33 includes an explicit foreign disclosure or release marking as required by Reference (m) for classified intelligence information under the purview of the DNI.

Figure 33. Examples of SCI Control Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

<u>Banner Line</u>	<u>Portion Marking</u>
TOP SECRET//HCS//NOFORN	(TS//HCS//NF)
SECRET//SI//TK//RELIDO	(S//SI//TK//RELIDO)
TOP SECRET//SI-GAMMA//ORCON//NOFORN	(TS//SI-G//OC//NF)
CONFIDENTIAL//SI//REL TO USA, AUS, FRA	(C//SI//REL TO USA, FRA)
TOP SECRET//SI-XXX//REL TO USA, AUS	(TS//SI-XXX//REL)
SECRET//HCS-O XYZ//NOFORN	(S//HCS-O XYZ//NF)
SECRET//TK-GEOCAP//NOFORN	(S//TK-G//NF)
SECRET//ABC//RELIDO	(S//ABC//SI//RELIDO)

d. Use a hyphen without interjected spaces to separate an SCI control system name and its compartment(s) when applicable, e.g., “SI-GAMMA,” or to separate multiple compartments from each other, e.g., “SI-G-XXX.” List multiple compartments alpha-numerically. In Figure 33, –GAMMA and –XXX are compartments of SI.

e. Separate sub-compartments from their compartment, and from each other if more than one, by a space (“ ”). List multiple sub-compartments alpha-numerically. In Figure 33, “XYZ” is a sub-compartment of the HCS compartment “O.”

f. When HCS or TK-GEOCAP is used, NOFORN must also be used.

g. SCI, regardless of classification level, must be processed only on an information system accredited for SCI processing (e.g., JWICS) and may not be processed, transferred to, or stored on SIPRNET, even if the information’s classification is at the SECRET level (e.g., SECRET//SI), as SIPRNET is not accredited for SCI. Any transfer or processing of SCI on SIPRNET constitutes a data spillage from a higher to a lower-security information domain, in accordance with Committee on National Security Systems Policy 18 (Reference (ad)). See Volume 3, Enclosures 6 and 7 for guidance on security violations and data spills.

7. SAP CONTROL MARKINGS

a. SAP control markings used in the banner line and at portions denote classified information that requires extraordinary protection in accordance with section 4.3 of Reference (d), DoDD 5205.07 (Reference (ae)), DoDI 5205.11 (Reference (af), Volume 4 of DoDM 5205.07, (Reference (ag)), and this Manual.

b. SAP information shall be marked in accordance with the security classification guide developed for each program and the guidance contained herein. If questions on marking guidance arise, the guidance in the program classification guide takes precedence so long as it conforms to the content, formatting, and syntax requirements of Reference (ag) and this Volume. The markings discussed here are not all inclusive, yet, they reflect the basic marking requirements for DoD SAP material.

c. The level of classification (e.g., Top Secret), the caveat “Special Access Required” or its acronym “SAR,” and the program nickname (e.g., BUTTER POPCORN) or code word (e.g., DAGGER) and the dissemination control (if assigned) will be annotated on the banner line at the head and foot of each document page or media containing SAP information. Assigned program identifiers (PIDs) (e.g., BP and RZD) will not be used in the banner line. A hyphen (-) without interjected spaces shall be used to separate “SAR” and the program’s nickname or code word. A slash (“/”) shall be used to separate nicknames or code words if more than one is required (see paragraph 7.e. of this section when citing three or more programs).

d. Each paragraph shall be portion marked with the level of classification, SAR, and the program’s assigned PID (e.g., TS//SAR-BP). Use a hyphen without interjected spaces to separate the “SAR” caveat and PID. List the PIDs alphabetically, separated by a slash, when there are multiple PIDs.

e. When information from three or more SAPs is included in a single document, indicate “MULTIPLE PROGRAMS” after SAR in the banner line (e.g., SECRET//SAR-MULTIPLE PROGRAMS). The term “Multiple Sources” is placed as the derivative classification instruction

on the first page and these multiple sources are listed at the end of the document. When there are multiple programs, the PID for each SAP must be cited in the portion marking, regardless of the total number of PIDs. Multiple PIDs must be listed in alphabetical order, separated from one another by a single forward slash (/), the SAR caveat, and PID. See Figure 34.

f. SAPs specifically exempted from normal Congressional reporting requirements by the Secretary of Defense shall also be marked “WAIVED” in the banner line, portion marks, and prominently on media (e.g., TOP SECRET//SAR-BP//WAIVED). In such cases, “WAIVED” is used as a dissemination control marking.

Figure 34. Examples of SAP Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

<u>Banner Line</u>	<u>Portion Marking</u>
TOP SECRET//SPECIAL ACCESS REQUIRED-BUTTERED POPCORN	(TS//SAR-BP)
TOP SECRET//SAR-SWAGGER	(TS//SAR-SGR)
TOP SECRET//TALENT KEYHOLE//SAR-BP	(TS//TK//SAR-BP)
TOP SECRET//SAR-BLUE FROG/ SAR-MUDDY PATH	(TS//SAR-BFG/SAR-MDP)
T Use “Multiple Programs” only when three or more SAPs are referenced in the document or portion	(TS//SAR-TG/SAR-STK/SAR-BP)
TOP SECRET//SAR-TIN BAKER//WAIVED	(TS//SAR-TB//WAIVED)
TOP SECRET//SAR-DAGGER//WAIVED	(TS//SAR-DGR//WAIVED)
SECRET//HVSACO	
UNCLASSIFIED//HVSACO	

g. Handle via Special Access Channels Only (HVSACO) is a control marking used within the DoD SAP community to convey handling instructions; it is not a classification level or dissemination control. HVSACO is applied to non-SAP material (unclassified or classified) that exists within a SAP environment and due to its subject or content warrants handling only within SAP channels, amongst SAP cleared personnel. Marking guidance for HVSACO material is conveyed in program classification guides.

h. The classification level, the caveat “Special Access Required,” and the program nickname will be noted on all document cover sheets. Annotating program code words on document cover sheets is prohibited.

i. SAP information, regardless of classification, shall be processed only on an information system accredited for SAP processing, and operating at a classification level that meets or exceeds the classification level of the SAP data.

j. DoD SAPs have been granted a file series exemption (FSE). This decision states that documents containing DoD SAP information are exempt from automatic declassification at 25 years and will, instead, be reviewed for declassification prior to December 31st of the year that is 50 years from the date of origin of the document. Accordingly, in addition to the other required information in the classification authority block, the DoD SAP community shall reflect this declassification guidance as shown at Figure 35 on all SAP documents.

Figure 35. Declassification Markings for SAP Information

<u>INFORMATION CLASSIFIED BY AN ORIGINAL CLASSIFICATION AUTHORITY</u>
<ul style="list-style-type: none"> For material dated <u>prior</u> to January 1, 1982 Declassify on: 25X[*], 20211231 Authority: FSE dtd 30 Mar 2005 For material dated <u>on or after</u> January 1, 1982 Declassify on: 25X[*], [insert 50th anniversary of the document] Authority: FSE dtd 30 Mar 2005 For material dated <u>on or after</u> April 30, 2015 Classified by: Name and position, agency if not apparent Reason: 1.4 [list appropriate subparagraph(s) a-h] Declassify on: [December 31st of the year document is 50 years old] Authority: FSE dated 20150306
<u>INFORMATION WHICH IS DERIVATIVELY CLASSIFIED</u>
<ul style="list-style-type: none"> For material dated <u>prior</u> to January 1, 1982 Declassify on: 25X[*], 20211231 Authority: FSE dtd 30 Mar 2005 For material dated <u>on or after</u> January 1, 1982 Declassify on: 25X[*], [insert 50th anniversary of the document] Authority: FSE dtd 30 Mar 2005 For material dated <u>on or after</u> April 30, 2015 Classified by: Name and position, agency if not apparent Derived from: SCG[date]; the source document, author and date, or Multiple Sources. Declassify on: [December 31st of the year document is 50 years old] Authority: FSE dated 20150306
* List appropriate 25X exemption code

8. ATOMIC ENERGY ACT INFORMATION MARKINGS. RD and FRD are not dissemination control markings, but instead they are unique categories of classified information defined by section 2014 of title 42, U.S.C. (also known and hereafter referred to as “The Atomic Energy Act of 1954, as amended”) (Reference (ah)). Program guidance is provided in subpart A, part 1045 of title 10, Code of Federal Regulations (Reference (ai)). Guidance on policies and procedures governing access to and dissemination of RD, including CNWDI and Sigma

categories, which are subsets of RD, and FRD by the DoD is provided by DoDI 5210.02 (Reference (aj)). DoDI 5210.83 (Reference (ak)) provides guidance on policies and procedures governing access to and dissemination of DoD unclassified controlled nuclear information (DoD UCNI).

a. RD

(1) RD includes all data concerning the design, manufacture, or utilization of nuclear weapons; the production of special nuclear material (SNM); or the use of SNM for production of energy. SNM includes plutonium, uranium-233, and uranium enriched in isotope 235.

(2) All RD information is excluded from the requirements of Reference (d). Section 6.2 of Reference (d) specifically excludes RD and FRD from the provisions of the Executive Order, stating such information shall be handled, protected, classified, downgraded, and declassified as required by provisions of The Atomic Energy Act of 1954, as amended and regulations issued under that Act. Automatic declassification of RD is prohibited.

(3) DOE manages government-wide RD classification and declassification systems.

(a) Only DOE may originally classify or declassify RD.

(b) Within the DoD, individuals with access to RD may derivatively classify RD.

(c) To the maximum extent practical, all RD documents shall be classified based on joint DOE-DoD classification guides. When use of classification guides is not practical, source documents may be used as the basis for classification.

(4) The RD marking shall be used only with TOP SECRET, SECRET, or CONFIDENTIAL.

(5) Use [classification]//RESTRICTED DATA (or RD) for the banner line. The portion marking is ([classification]//RD). If any portion of the document contains RD information, RD must appear in the banner line.

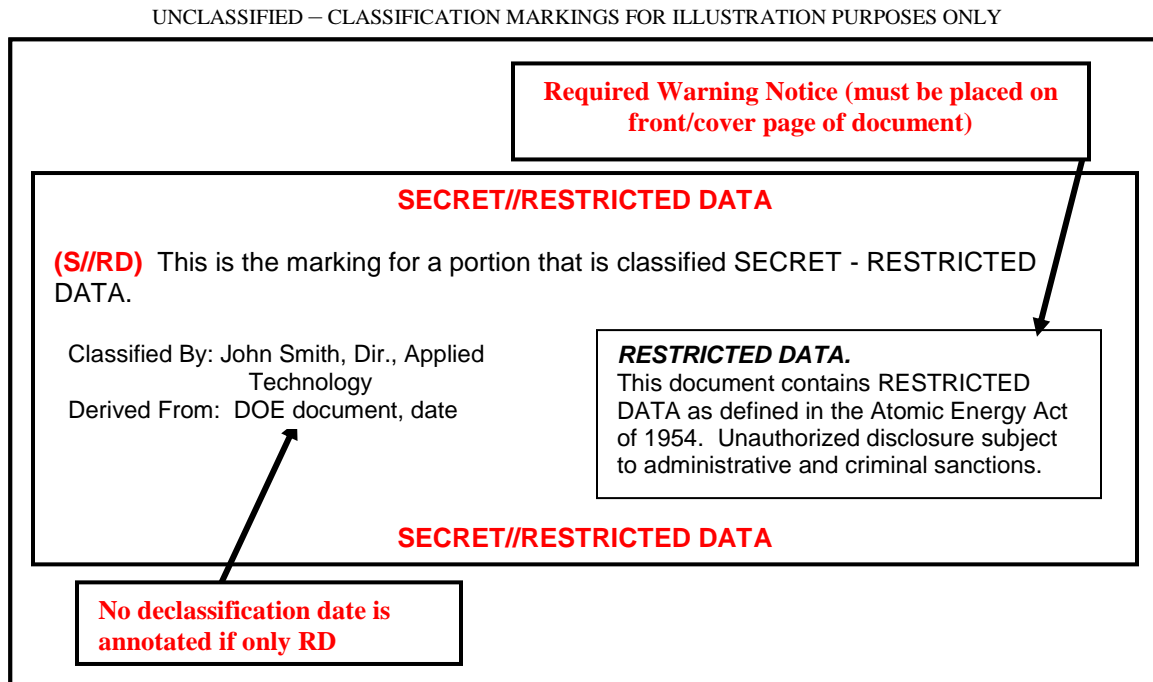
(6) RD documents shall be marked with the identity of the derivative classifier ("Classified By:") and shall include a "Derived From:" line which shall identify the guide(s) or source document(s), by title and date, used to classify the document.

(7) RD is not subject to automatic declassification. Therefore, a declassification instruction is never annotated on documents containing solely RD information. The "Declassify On:" line shall state "Not applicable" or may be deleted. (See paragraph 8.a.(10) of this section if a document contains both RD and NSI.)

(8) Although documents originated in other agencies and containing RD information may not be portion marked, DoD-originated documents containing RD information require portion marking.

(9) All documents containing RD information shall carry a warning notice on the face of the document as shown in Figure 36. Unclassified transmittal documents containing no RD shall be marked with a statement similar to this: “Document transmitted herewith contains [classification] RESTRICTED DATA.” The full notice shall appear on the face of the transmitted document.

Figure 36. Example of RD Markings



(10) To the greatest degree possible, do not commingle RD in the same document with information classified pursuant to Reference (d) (i.e., NSI). When mixing cannot be avoided, the requirements of this paragraph must be met.

(a) Do not commingle RD and NSI in the same portion. Portions containing RD and NSI must be clearly delineated using the markings specified in this Volume.

(b) The “Declassify On:” line shall be annotated “Not Applicable (or N/A) to RD/FRD portions” and “See source list for NSI portions.” The source list shall include the declassification instruction for each source classified pursuant to Reference (d). The source list and declassification instructions shall NOT appear on the front page or cover of the document.

(c) If an NSI portion is extracted for use in a derivative document, the declassification date for the extracted portion shall be determined using the source list, the applicable classification guide, or consultation with the OCA. If the original, commingled document is not portion marked, it may not be used for derivative classification.

b. FRD

(1) FRD is information removed from RD upon a joint determination by the Departments of Defense and Energy that the information relates primarily to military utilization of atomic weapons. The Departments have joint responsibility for originally classifying or declassifying FRD.

(a) Within the DoD, individuals with access to FRD may derivatively classify FRD.

(b) The ONLY approved source documents for derivative classification of FRD are the joint DOE/DoD security classification guides. Cite the security classification guide on the “Derived from:” line.

(2) FRD shall be used only with TOP SECRET, SECRET, or CONFIDENTIAL.

(3) Use [classification]//FORMERLY RESTRICTED DATA (or FRD) for the banner line. The portion marking is ([classification]//FRD). If any portion of the document contains FRD information, FRD must appear in the banner line.

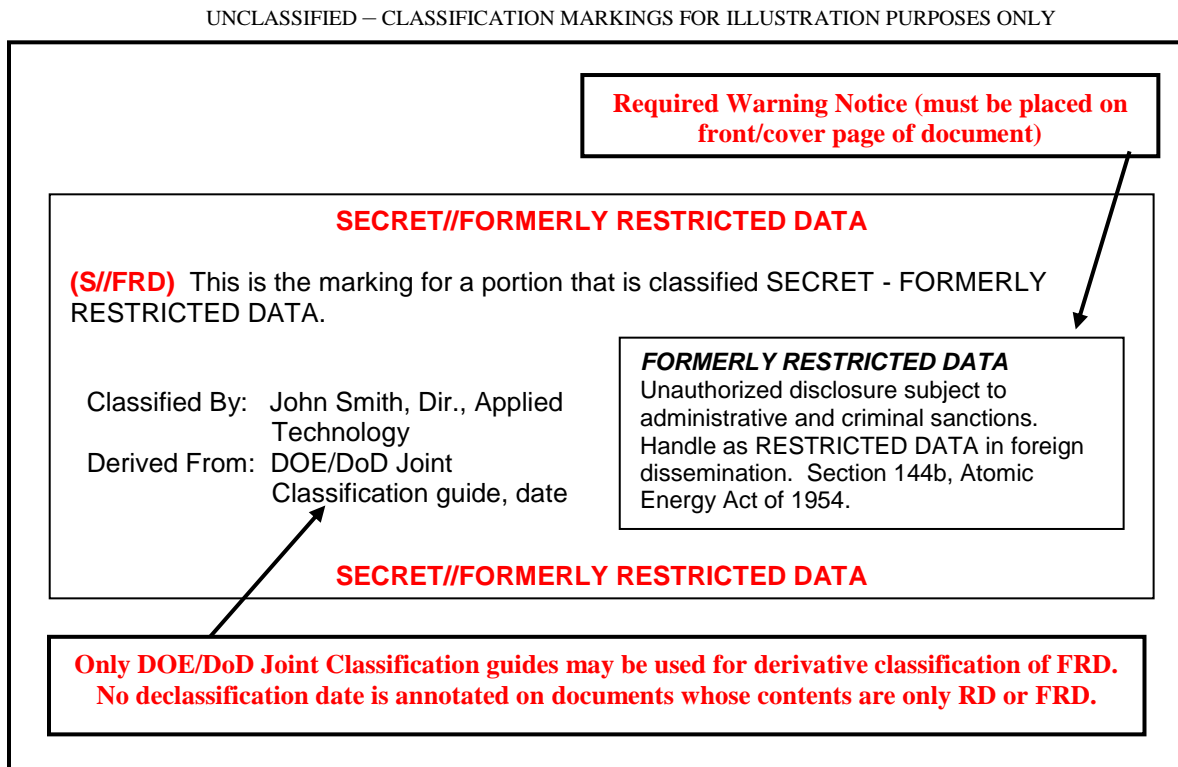
(4) FRD documents shall be marked with the identity of the derivative classifier (“Classified By:”) and shall include a “Derived From:” line in accordance with subparagraph 8.b(1)(b) of this section.

(5) FRD is excluded from the provisions of Reference (d) and is not subject to automatic declassification. Therefore, a declassification date is never annotated on documents containing only FRD. The “Declassify On:” line shall state “Not applicable” or may be deleted. (See paragraph 8.b.(8) of this section if a document contains both FRD and NSI.)

(6) DoD documents containing FRD shall be portion marked.

(7) All documents containing FRD, but no RD, shall carry a warning notice on the face of the document as shown in Figure 37. If the document also contains RD, use the notice shown in Figure 36. Unclassified transmittal documents containing no FRD shall be marked with a statement similar to this: “Document transmitted herewith contains [classification] FORMERLY RESTRICTED DATA.” The full notice shall appear on the face of the transmitted document.

Figure 37. Example of FRD Markings



(8) To the greatest degree possible, do not commingle FRD in the same document with information classified pursuant to Reference (d) (i.e., NSI). When mixing cannot be avoided, the requirements of this paragraph must be met.

(a) Do not commingle FRD and NSI in the same portion. Portions containing FRD and NSI must be clearly delineated using the markings specified in this Volume.

(b) The “Declassify On:” line shall be annotated “Not Applicable (or N/A) to RD/FRD portions” and “See source list for NSI portions.” The source list shall include the declassification instruction for each source document classified pursuant to Reference (d). The source list and declassification instructions shall NOT appear on the front page or cover of the document.

(c) If an NSI portion is extracted for use in a derivative document, the declassification date for the extracted portion shall be determined using the source list, the applicable classification guide, or consultation with the OCA. If the original, commingled document is not portion marked, it may not be used for derivative classification.

c. CNWDI

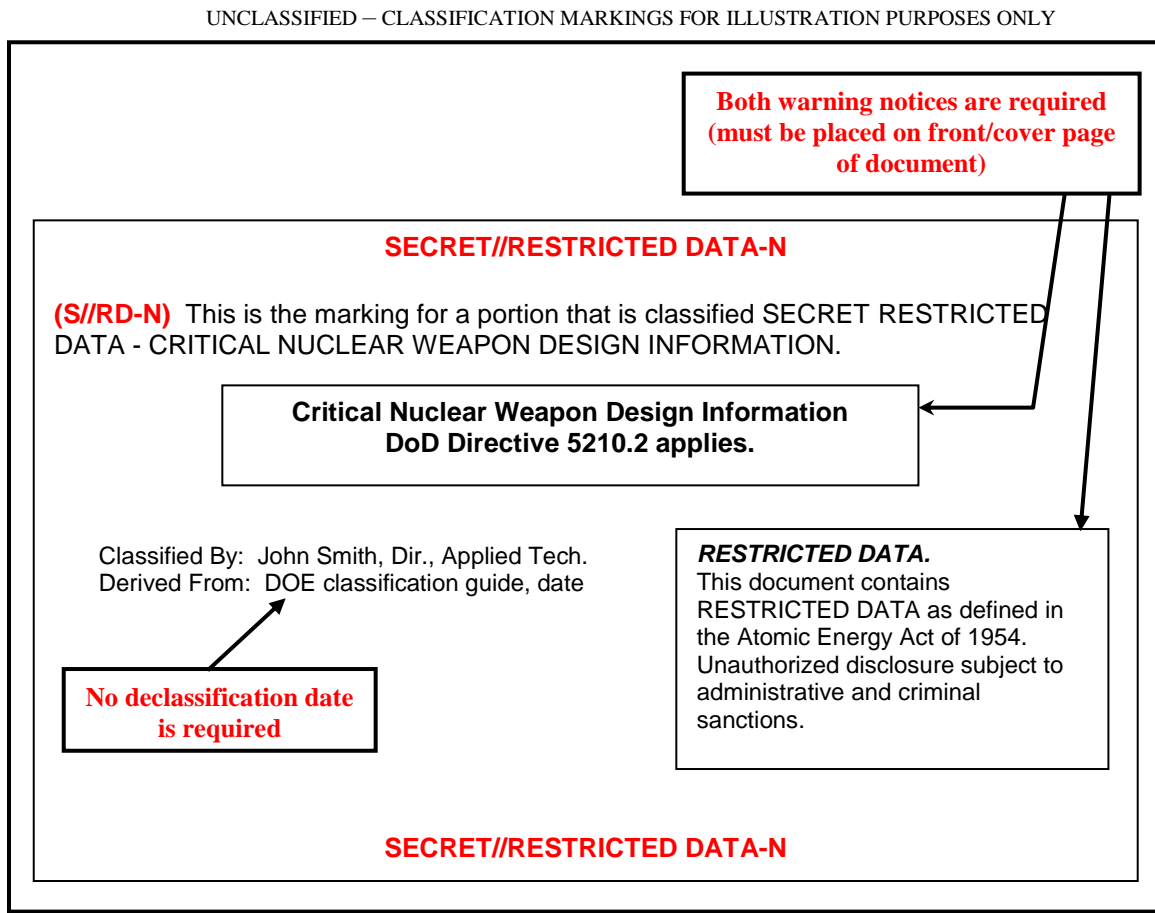
(1) CNWDI is the DoD designation for TOP SECRET RD or SECRET RD weapons data that reveals the theory of operation or design of the components of a thermonuclear or

fission bomb, warhead, demolition munitions, or test device. The designation CNWDI specifically excludes information concerning arming, fusing, and firing systems; limited-life components; and total contained quantities of fissionable, fusionable, and high-explosive materials by type.

(2) Access to CNWDI is on a need-to-know basis and a special DoD briefing is required. See Reference (ad) for further guidance.

(3) As CNWDI is a subset of RD, use the same rules for marking CNWDI information as for marking RD, except “-N” shall be appended to the banner and portion markings, as shown in Figure 38. Additionally, add the CNWDI warning notice shown in Figure 38 to the face of the document.

Figure 38. Example of CNWDI Markings



d. Sigma

(1) Sigma categories identify RD and/or FRD that concern the design, manufacture, or utilization of atomic weapons or nuclear explosive devices.

(2) The SIGMA marking shall be used only with TOP SECRET, SECRET, or CONFIDENTIAL.

(3) The required format of classification banner markings is: [classification]//[RD or FRD]-SIGMA [#]. The [#] represents the Sigma number which may be between 1 and 99. If multiple SIGMAs apply, list them in numerical order, separated with a space (“ ”) (see Figure 39). Use “SG” with the Sigma number in the portion marking.

(4) Apply the appropriate RD or FRD warning notice (see Figure 36 or 37 for wording of the applicable notice) to the face of the document.

(5) Sigma 14 information must additionally be marked with the handling instruction shown in Figure 40.

Figure 39. Example of SIGMA Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//RD-SIGMA 1 2

(S//RD-SG 1) This is the marking for a portion that is classified SECRET - RESTRICTED DATA, SIGMA 1.

(S//RD-SG 2) This is the marking for a portion that is classified SECRET - RESTRICTED DATA, SIGMA 2.

~~Classified By: John Smith, Dir, Applied Tech~~
~~Derived From: DOE classification guide, date~~

RESTRICTED DATA.
This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

SECRET//RD-SIGMA 1 2

Required warning notice (must be placed on front/cover page of document)

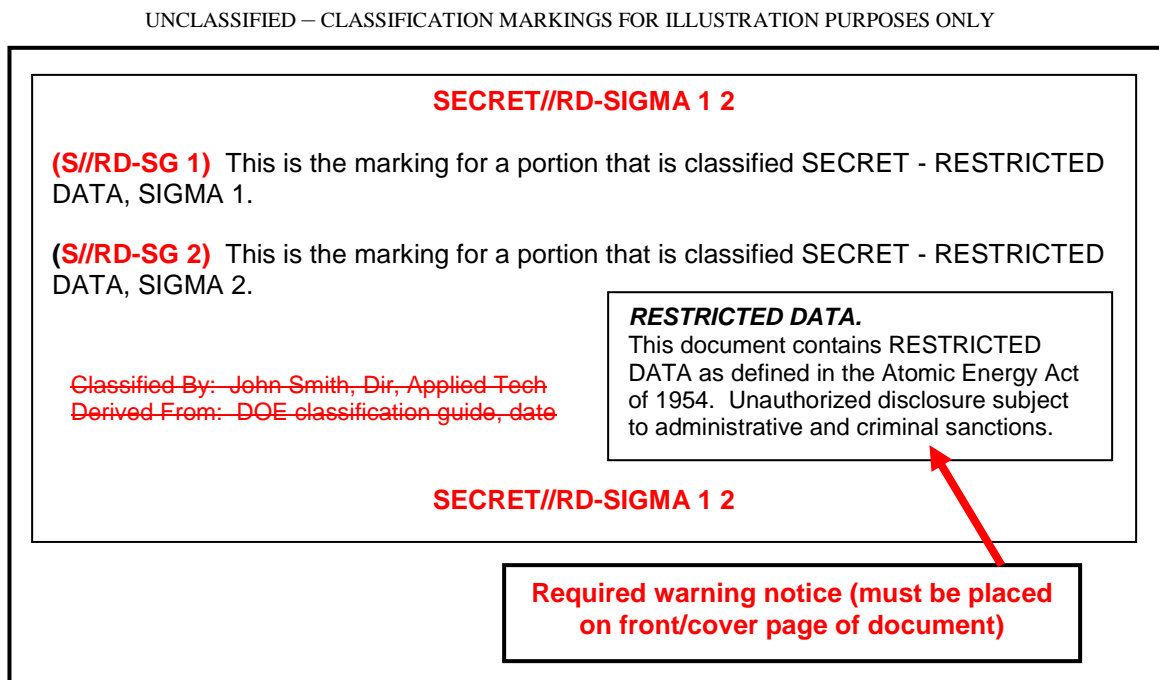
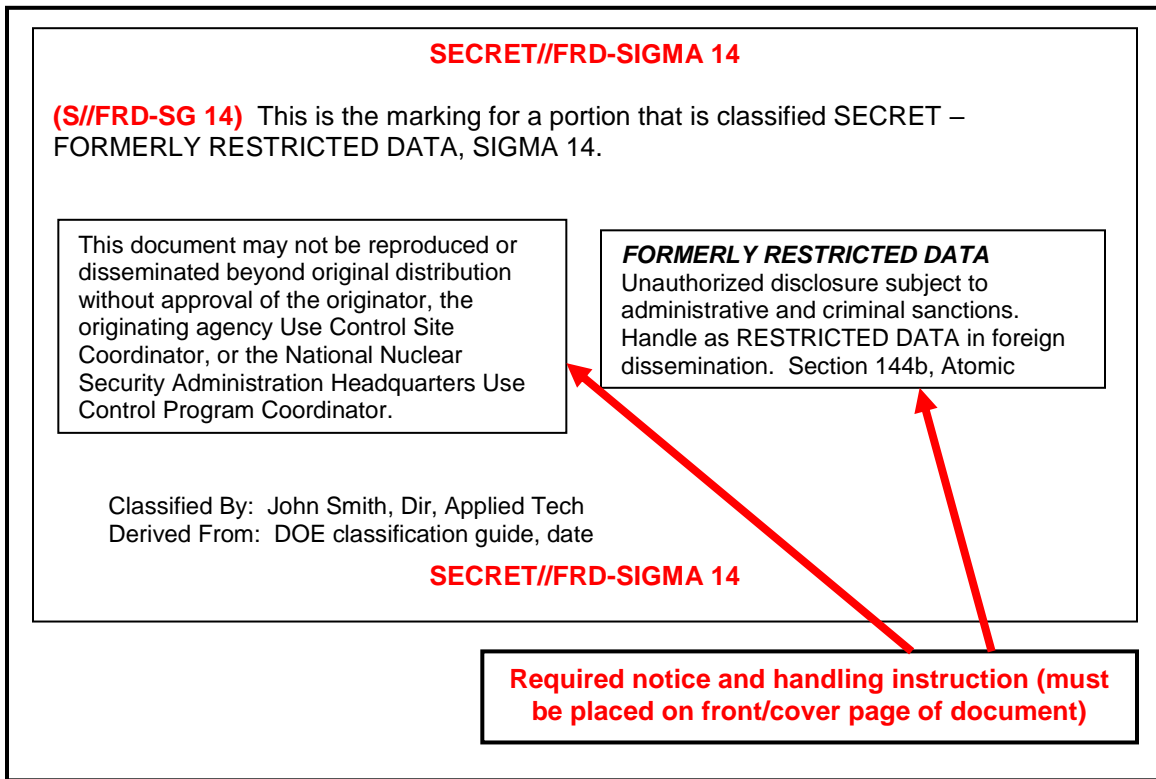


Figure 40. Example of SIGMA 14 Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



9. FGI MARKINGS USED IN U.S. DOCUMENTS

a. FGI markings are used in U.S. products to denote the presence of foreign-controlled information. These markings are used based on treaties, sharing agreements or arrangements with the source country or international organization and are necessary to provide a degree of protection at least equivalent to that required by the foreign government or international organization that furnished the information, and to prevent premature declassification or unauthorized disclosure. (See section 4 of this enclosure for markings to be used on documents that consist entirely of FGI.)

b. As damage to the national security is the criteria for classification, FGI requiring protection from disclosure must automatically be classified at a level no less than CONFIDENTIAL, unless otherwise noted in security agreements between the security authorities of the United States and the applicable foreign government.

c. Use FGI markings when FGI is included in a U.S.-controlled document (see Figures 41 through 44).

d. Except as provided in paragraph 9.e. of this section, use “FGI” with the trigraphic country codes and international organization tetragraphs in the banner line; portion markings for included FGI shall be as specified in section 4 of this enclosure. If multiple governments and/or

international organizations furnished information, the country trigraphs shall be listed in alphabetical order followed by the international tetragraphs in alphabetical order, each separated by a single space.

Figure 41. Example of FGI Marking

TOP SECRET//FGI DEU GBR

(TS) This is the marking for a portion which is classified TOP SECRET. This portion shall contain only US classified information.

(//DEU S) This is the marking for a German SECRET portion within a US classified document. This portion shall contain only German SECRET FGI.

(//GBR U) This is the marking for a British UNCLASSIFIED portion within a US classified document. This portion shall contain only British UNCLASSIFIED FGI.

Classified By: J. Jones, Dir., Ofc of Good Works
Derived From: Multiple Sources
Declassify On: 20321215

TOP SECRET//FGI DEU GBR

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Figure 42. Example of FGI Marking with NATO Information

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

TOP SECRET//FGI DEU GBR NATO

(C) This is the marking for a portion which is classified CONFIDENTIAL. This portion shall contain only US classified information.

(//DEU S) This is the marking for a German SECRET portion within a US classified document. This portion shall contain only German SECRET FGI.

(//GBR S) This is the marking for a British SECRET portion within a US classified document. This portion shall contain only British SECRET FGI.

(//CTS) This is the marking for a NATO COSMIC TOP SECRET portion within a US classified document. This portion shall contain only NATO COSMIC TOP SECRET FGI.

Classified By: T. Smith, Pgm Mgr
Derived From: Multiple Sources
Declassify On: 25X9, 20571215

THIS DOCUMENT CONTAINS
NATO TOP SECRET INFORMATION

TOP SECRET//FGI DEU GBR NATO

Figure 43. Example of FGI Marking When Originating Country Is Concealed

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//FGI

(S) This is the marking for a portion which is classified SECRET. This portion shall contain only U.S. classified information.

(//DEU S) This is the marking for a German SECRET portion within a U.S. classified document. This portion shall contain only German SECRET FGI.

(//FGI S) This is the marking for a portion which is FGI classified SECRET in cases where the originating country must be concealed within a U.S. classified document. This portion shall contain only SECRET FGI from that single, originating country. The banner line specifies only FGI as it is the most restrictive marking.

Classified By: T. Smith, Pgm Mgr
 Derived From: Memorandum XYZ,
 Dated 20071215
 Declassify On: 20321215

SECRET//FGI

Figure 44. Example of FGI Marking with REL TO

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

TOP SECRET//FGI CAN DEU

(S//REL TO USA, AUS) This is the marking for a portion that is releasable to Australia within a U.S. classified document. This portion shall contain only U.S. classified information that is releasable to Australia.

(//CAN S//REL TO USA, AUS, CAN, GBR) This is the marking for a Canadian SECRET portion for which Canada has allowed release back to Canada and further release to Australia and Great Britain within a U.S. classified document. This portion shall contain only Canadian SECRET FGI releasable to those countries listed.

(//DEU TS) This is the marking for a German TOP SECRET portion within a U.S. classified document. This portion shall contain only German TOP SECRET FGI.

Classified By: T. Smith, Pgm Mgr
 Derived From: Memorandum XYZ,
 Dated 20071215
 Declassify On: 20321215

TOP SECRET//FGI CAN DEU

e. In cases where one or more specific government(s) must be concealed, do not include country codes within the banner or applicable portion marking(s). In such cases, the applicable portion marking shall be “FGI” together with the appropriate classification (e.g., //FGI S). If the

very fact that the information is FGI must be concealed, the information shall be marked as if it were wholly of U.S. origin. In both cases the identity of the foreign government shall be maintained with the record copy, which must be appropriately protected.

f. In documents containing FGI, the FGI portion(s) shall remain segregated from the U.S. portions.

g. In documents containing FGI from more than one country and/or international organization, the FGI from each individual country or international organization shall remain segregated in separate portions.

h. Release or disclosure of FGI back to the source country is implied, unless otherwise indicated.

i. The release or disclosure of FGI to any third-country entity, including foreign nationals who are protected individuals or permanent resident aliens, or to any third party, or use for other than the purpose for which the foreign government provided the information requires the prior written consent of the originating government when required by treaty, agreement, bilateral exchange, or other obligation. Questions regarding releasability or disclosure should be directed to the U.S. originator, who will consult with the foreign government as required.

j. When FGI is included in a U.S. document, the overall U.S. classification used shall reflect the highest classification of any information, including the FGI, in the document.

k. FGI and NOFORN in the banner line signals that the document may not be disseminated to any foreign country without the permission of the U.S. originator and the source country providing the FGI. Releasability of individual portions shall be in accordance with their markings. Questions regarding releasability or disclosure should be directed to the U.S. originator, who will consult with the foreign government as required.

l. REL TO cannot be used in the overall classification of a document containing FGI portions unless the entire document is releasable to all countries listed. When both NOFORN and REL TO information are included in the same document, NOFORN takes precedence over REL TO.

m. Portion marks for portions containing FGI may not include "NOFORN." NOFORN is a U.S. marking and is not applicable to portions containing only FGI. Release limitations, per paragraph 9.i of this section, are implied by the FGI designation.

n. Unclassified FGI is withheld from public release until approved for release by the source country.

o. The "Derived From:" line or source list shall identify U.S. as well as foreign classification sources. If the identity of the foreign government (but not the fact of FGI content) must be concealed and citation of the source would reveal that identity, the "Derived From:" line or source list shall contain the notation, "FGI source" and, where possible, the date of the

document. The originator shall maintain the full source citation and the identity of the foreign government with the record copy and protect it as Volume 3, Enclosure 2 of this Manual requires.

p. A U.S. document marked as described herein shall not be downgraded below the highest level of FGI contained in the document or be declassified without the written approval of the foreign government that originated the information. Submit recommendations concerning downgrading or declassification to the DoD organization that created the document. If that organization supports the recommendation, it shall consult with the originating foreign government to determine whether that government consents to declassification. (See also Volume 1, Enclosure 5, section 20 of this Manual.)

10. DISSEMINATION CONTROL MARKINGS

a. Dissemination Control Markings for Intelligence Information. Certain dissemination control markings are authorized for use only on intelligence information. Among these are “NOFORN” (with exceptions for NNPI and NDP-1), cover and cover support information in accordance with Reference (y), “RELIDO,” and “IMCON.” As provided in paragraph 1.d of Enclosure 2 of this Volume, DoD Intelligence Components shall refer to policy and implementing guidance issued by the DNI for guidance on marking intelligence and intelligence-related information and products under the purview of the DNI. Information on intelligence control markings is contained in Appendix 2 to this enclosure to assist other DoD activities that may encounter such markings in understanding their meaning and use.

b. FOUO

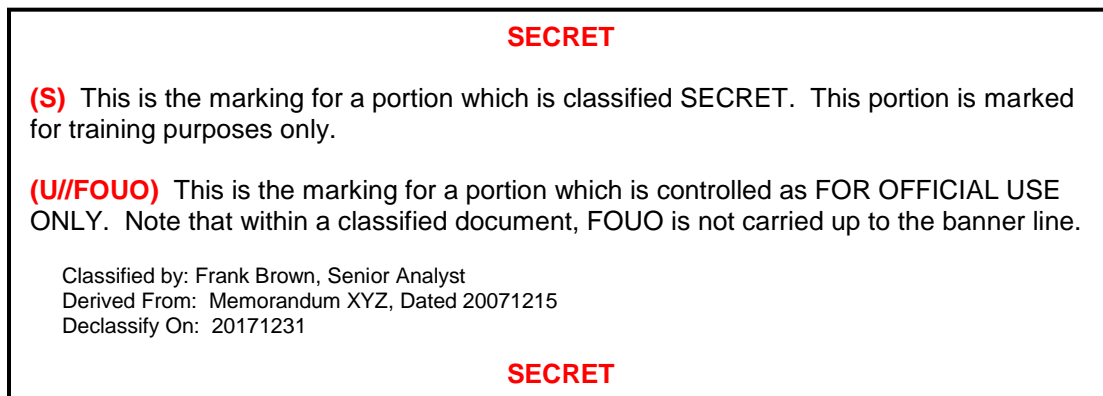
(1) Within the DoD, FOUO is a control marking for unclassified information that may be withheld from the public if disclosure would reasonably be expected to cause a foreseeable harm to an interest protected under the Freedom of Information Act. The use of FOUO markings shall remain in effect until the revised Volume 4 of this Manual is published.

(2) FOUO is also used by other agencies to protect certain types of unclassified information. FOUO from other agencies is treated the same as DoD FOUO information.

(3) FOUO portions within a classified document shall be marked (U//FOUO); however, FOUO shall not appear in the overall classification banner because the classification adequately protects the unclassified information, except when page markings are used to reflect the classification of information on that page instead of the overall document classification (see Figure 47). In that case, the banner line for unclassified pages with FOUO information shall be: UNCLASSIFIED//FOR OFFICIAL USE ONLY or UNCLASSIFIED//FOUO.

Figure 45. Example of FOUO Marking in a Classified Document

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



b. Controlled Unclassified Information (CUI)

(1) Within the DoD, CUI is a control marking for unclassified information the Government creates or possesses (or that an entity creates or possesses for or on behalf of the Government) that a law, regulation or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls in accordance with Volume 4 of this Manual.

(2) Consult Volume 4 of this Manual for guidance on markings required for unclassified documents containing CUI and the exemption notice required on documents containing CUI distributed outside the DoD.

(3) Consistent with Reference (m), REL TO and RELIDO may be applied, when warranted, to unclassified intelligence or other information that has been determined to be properly categorized as CUI.

c. Dissemination and Extraction of Originator Controlled (ORCON) Information

(1) The ORIGINATOR CONTROLLED or ORCON marking is used when dissemination and extraction of information must be controlled by the originator.

(a) ORCON may be used by the DoD Components to mark information that requires the originator's consent for further dissemination or extraction of information when the classification level and other controls alone are insufficient to control dissemination. ORCON is to be applied sparingly as its use impedes efficient information sharing. The decision to apply the ORCON marking shall be made on a case-by-case basis using a risk management approach; it may not be applied in a general or arbitrary manner.

(b) ORCON is authorized for use by the DoD Components that are elements of the IC for classified intelligence that clearly identifies or reasonably permits ready identification of intelligence sources or methods that are particularly susceptible to countermeasures that would negate or measurably reduce their effectiveness. ORCON may be used with national

intelligence, which is under the purview of the DNI, only as described in ICPG 710.1 (Reference (am)) and DNI Memorandum (Reference (an)).

(2) Information bearing the ORCON marking may be disseminated within the recipient agency and its subordinate elements, including to contractors located within government facilities, without further approvals consistent with any other dissemination control markings. Such information may also be incorporated in whole or in part into briefings or other products, provided the briefing or product is presented or distributed only to original recipients of the information. Dissemination beyond the recipient agency or to agencies other than the original recipients requires advance permission from the originator. For purposes of this section, DoD is considered one agency except with respect to information disseminated by IC elements in accordance with DNI guidelines. This information may only be further disseminated by recipient DoD components to the organizations identified in the originators dissemination/distribution list.

(3) ORCON may be used with TOP SECRET, SECRET, or CONFIDENTIAL.

(4) Use [classification]//ORCON for the banner line. The portion marking for ORCON is ([classification]//OC) (see Figure 45). If any portion is ORCON, ORCON must appear in the banner line.

(5) The originator shall include a point of contact who can make ORCON release determinations on all information marked ORCON. Include, at a minimum, name or position title of the contact and a current telephone number.

(6) The originator shall promptly review all requests for further dissemination of ORCON information. A determination shall be provided to the requestor, normally within 3 days of receipt of the request, but not more than 7 days, unless justification for a longer time is provided to the recipient within 7 days. Release determinations shall be formally documented; documentation shall include the request justification and identification of recipients. Where requests have been denied, the documentation shall include justification for the denial which articulates the risks of further dissemination and why those risks outweigh the need to share.

Figure 46. Example of ORCON Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

TOP SECRET//ORCON//NOFORN

(TS//OC/NF) This is the marking for a portion which is classified as TOP SECRET ORIGINATOR CONTROLLED. In accordance with ICD 710, a foreign disclosure marking (NOFORN) is included. This portion is marked for training purposes only.

Classified By: J. Jones, Dir., Dept of Good Works
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

TOP SECRET//ORCON//NOFORN

d. Authorized For Release To (REL TO)

(1) Within the DoD, the AUTHORIZED FOR RELEASE TO or REL TO control marking is authorized for use on all classified military or Defense CUI information that has been determined by an authorized disclosure official, in accordance with established foreign disclosure policies, to be releasable, or that has been released through established foreign disclosure procedures and channels, to the foreign country and/or international organization indicated. Figures 46 through 48 provide examples of the use of the REL TO marking.

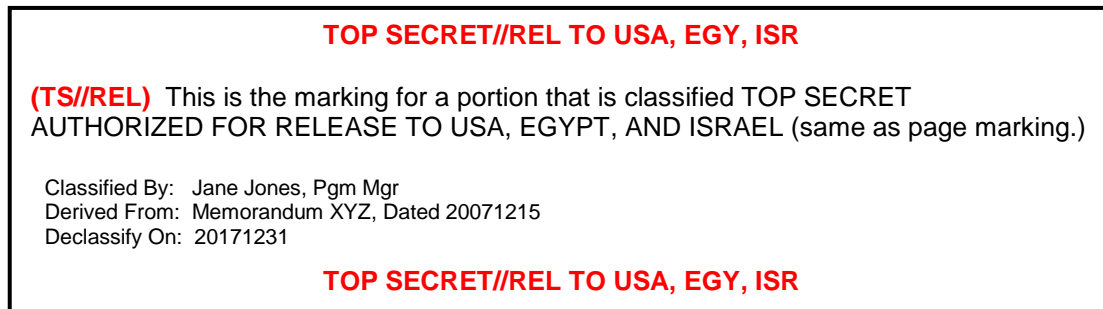
(2) Foreign release or disclosure of the material, in any form, to the nations specified in the REL TO marking is authorized without originator approval. Disclosure to nations not specified in the REL TO marking is authorized only after obtaining permission from the originator.

(3) REL TO shall be used with TOP SECRET, SECRET, CONFIDENTIAL, or CUI.

(4) The format for REL TO banner and portion markings is [classification]//REL TO [country codes]. Trigraphic country codes shall be listed first (USA first, followed by other countries in alphabetical order), followed by coalition or international organization tetragraph codes in alphabetical order. Each code shall be separated from the next by a comma and space.

Figure 47. Example of REL TO Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



(5) “USA” attached to “REL TO” means that the information is U.S.-originated and may be released to U.S. citizens who meet the standards for access to classified information and the restrictions imposed by any other caveats and who have a need to know. “REL TO USA” without any other countries listed is not an approved marking.

(6) The portion marking “REL” may be used when the countries to which the portion-marked information is releasable are the same as the countries listed in the REL TO in the banner line. If countries are different, the portion marking must list all countries that are applicable.

(7) REL TO shall not be used with NOFORN in the banner line. When a document contains both NOFORN and REL TO portions, use NOFORN in the banner line.

(8) REL TO should be used in the banner line only when the entire document is releasable to the countries listed. Otherwise, information not authorized for release may be inadvertently released. Users should additionally note that there is differing guidance between the DoD and the IC on the overall classification of a classified document containing both REL TO information and information without either REL TO, RELIDO or NOFORN markings (hereinafter referred to as “uncaveated information”) and on the treatment of documents where there is no common country listed throughout the REL TO portions.

(a) Within the DoD, except for national intelligence information under the control of the Defense Intelligence Components, if a document contains portions with REL TO markings and portions with uncaveated information, the banner line shall contain only the U.S. classification (e.g., SECRET). Additionally, for documents containing REL TO portions, if the document is not fully releasable to at least one country other than USA (i.e., there is no common country listed throughout the document’s portions), the banner line shall reflect, in addition to any other required caveats, simply the U.S. classification (i.e., the banner line shall not contain the REL TO marking). This marking standard shall be applied by the Defense Intelligence Components when the information is military intelligence.

Figure 48. Example of REL TO Marking When Not All Portions Are Equally Releasable

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//REL TO USA, NZL, NATO

(S//REL TO USA, JPN, NZL, NATO) This is the marking for a portion that is classified SECRET AUTHORIZED FOR RELEASE TO USA, Japan, New Zealand and NATO. Note that the entire document is releasable to USA, NZL, and NATO, but this paragraph is releasable to those countries plus JPN

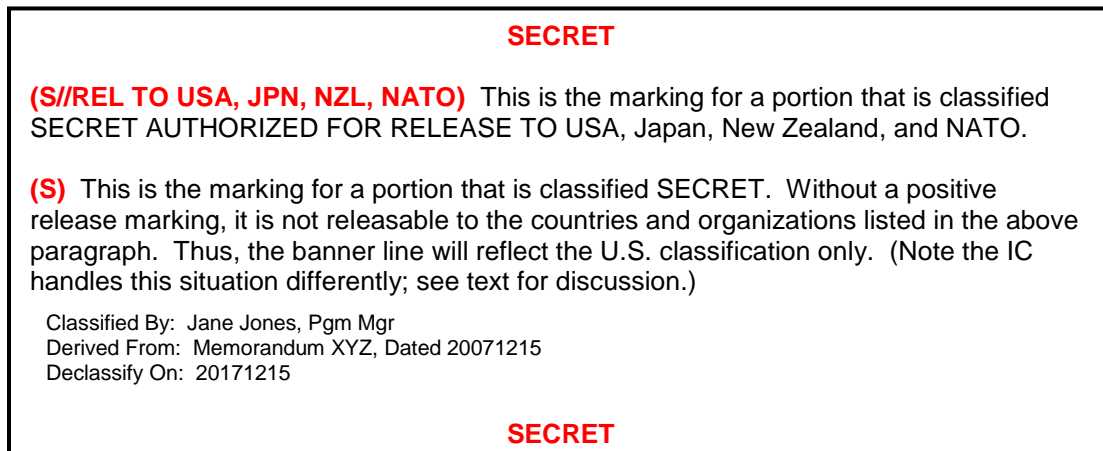
(S//REL) This is the marking for a portion that is classified SECRET AUTHORIZED FOR RELEASE TO USA, New Zealand and NATO (the same as the page markings.)

Classified By: Jane Jones, Pgm Mgr
 Derived From: Memorandum XYZ, Dated 20071215
 Declassify On: 20321215

SECRET//REL TO USA, NZL, NATO

Figure 49. Example of REL TO Marking When Portions Lack Explicit Release Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



(b) Reference (m) requires intelligence under the purview of the DNI to be explicitly marked for foreign release. A combination of REL TO and uncaveated national intelligence information (i.e., information under the purview of the DNI) is to be marked as NOFORN in the banner line (e.g., SECRET//NOFORN). Likewise, where there is no common country listed in the REL TO portions, NOFORN is to be applied in the banner line. As NOFORN may be used only on intelligence information, this IC practice is not permitted for DoD organizations that are not elements of the IC.

e. Display Only

(1) This dissemination control identifies classified information authorized for disclosure WITHOUT PROVIDING THE RECIPIENT A COPY FOR RETENTION, regardless of medium, through established foreign disclosure channels to the foreign country and/or international organization indicated. In accordance with ICPG 710.1 (Reference (ao)), disclosure is showing or revealing classified information, whether orally, in writing or via any other medium, without providing the recipient with a copy of the information for retention.

(2) Display Only information must remain under U.S. control at all times.

(3) The marking may be used with TOP SECRET, SECRET or CONFIDENTIAL.

(4) DISPLAY ONLY may not be used with RELIDO or NOFORN. Additionally, DISPLAY ONLY shall NOT be used with other dissemination control markings (e.g., REL TO) in either the portion or banner line, unless authorized by other policy guidance and established sharing arrangements and procedures.

(5) The format for Display Only banner and portion markings is [classification]//DISPLAY ONLY [country codes] (see Figure 49). Trigraphic country codes shall be listed first in alphabetical order followed by coalition or international organization

tetragraph codes in alphabetical order. Each code shall be separated from the next by a comma and space.

(6) DISPLAY ONLY appears in the banner line only if ALL portions are authorized for DISPLAY ONLY to the same list of countries. REL TO and DISPLAY ONLY may appear in the same banner line only if EVERY portion is authorized for REL TO [same country list] and DISPLAY ONLY [same country list] (see Figures 50, 51, and 52).

(7) Within a portion, DISPLAY ONLY can be used in conjunction with REL TO only when all information within the portion has been reviewed through the originator's foreign disclosure channels and approved for disclosure and release, as applicable, to the listed countries or international organizations and coalitions.

(8) IC organizations apply a warning statement, generally on the first page, when derivative use of DISPLAY ONLY information or release to other countries or international organizations is prohibited without authorization from the originating agency. Remove the warning statement when authorization for derivative use is received from the originating organization.

Figure 50. Example of DISPLAY ONLY Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//DISPLAY ONLY AFG

(S//DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET and authorized for DISPLAY ONLY to Afghanistan.

(S//DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET and authorized for DISPLAY ONLY to Afghanistan.

CLASSIFIED BY: K. Green, MG, USA, CMDR, TF ZULU
REASON: 1.4(b), 1.4(d)
DECLASSIFY ON: 20361231

SECRET//DISPLAY ONLY AFG

Figure 51. Example of DISPLAY ONLY Marking with REL TO

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//REL TO USA, GBR/DISPLAY ONLY AFG

(S//REL TO USA, GBR/DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET, authorized for release to the U.S. and United Kingdom, and authorized for DISPLAY ONLY to Afghanistan.

(S//REL TO USA, GBR/DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET, authorized for release to the U.S. and United Kingdom, and authorized for DISPLAY ONLY to Afghanistan. REL TO and DISPLAY ONLY appear in the banner line because all portions carry the same markings, to include the same country lists.

CLASSIFIED BY: K. Green, MG, USA, CMDR, TF ZULU
REASON: 1.4(b), 1.4(d)
DECLASSIFY ON: 20361231

SECRET//REL TO USA, GBR/DISPLAY ONLY AFG

Figure 52. Example of DISPLAY ONLY Marking When Not All Portions are DISPLAY ONLY

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//REL TO USA, GBR

(S//REL TO USA, GBR/DISPLAY ONLY AFG) This is the marking for a portion which is classified SECRET, authorized for release to the U.S. and United Kingdom, and authorized for DISPLAY ONLY to Afghanistan.

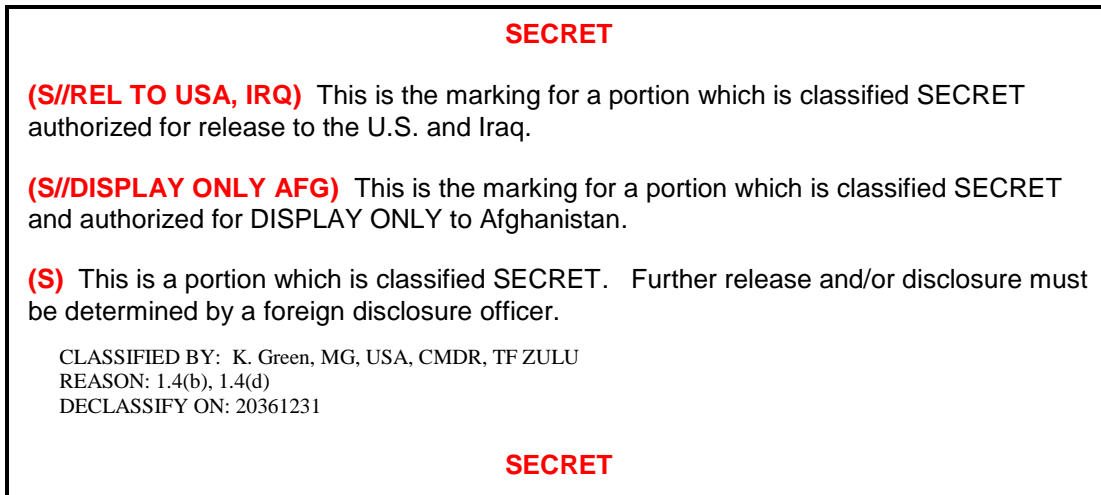
(S//REL TO USA, GBR) This is the marking for a portion which is classified SECRET, authorized for release to the U.S. and United Kingdom.

CLASSIFIED BY: K. Green, MG, USA, CMDR, TF ZULU
REASON: 1.4(b), 1.4(d)
DECLASSIFY ON: 20361231

SECRET//REL TO USA, GBR

Figure 53. Example of DISPLAY ONLY Marking In Mixed Releasability Situation

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



11. OTHER DISSEMINATION CONTROL MARKINGS. The dissemination control markings in this section fall into the “OTHER DISSEM” category in the marking syntax (CLASSIFICATION//SCI//SAP//AEA//FGI//DISSEM//OTHER DISSEM) and follow all previously discussed markings when used.

a. Alternative Compensatory Control Measures (ACCM)

(1) ACCM are security measures used to safeguard classified intelligence or operations when normal measures are insufficient to achieve strict need-to-know controls and where SAP controls are not required. See Enclosure 2 of Volume 3 of this Manual for current guidance on use of ACCM.

(2) The banner marking for each page of ACCM-protected information shall be the overall classification, the caveat “ACCM,” and the program’s nickname. Use a hyphen (-) without interjected spaces to separate the “ACCM” caveat and the program’s nickname (e.g., SECRET//ACCM-FICTITIOUS EFFORT). If more than one nickname is used, separate them by a forward slash (/) (e.g., SECRET//ACCM-FICTITIOUS EFFORT/TEA LEAF). Figure 59 provides an example of these markings.

Figure 54. Example of ACCM Markings

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//ACCM-FICTITIOUS EFFORT/TEA LEAF

(S//ACCM) This is the marking for a portion which is SECRET ACCM-protected information with the nicknames “FICTITIOUS EFFORT” and “TEA LEAF” (same as banner marking).

(S//ACCM-TEA LEAF) An ACCM-protected portion requiring only the nickname “TEA LEAF” would be marked as shown in this paragraph.

(S//ACCM-FICTITIOUS EFFORT) This is the marking for a portion which is SECRET ACCM-protected information requiring only the nickname “FICTITIOUS EFFORT.”

Classified By: Tom Brown, Chief, Tea Leaf Program Ofc
 Derived From: Memorandum XYZ, Dated 20071215
 Declassify On: 20121215

SECRET//ACCM-FICTITIOUS EFFORT/TEA LEAF

(3) ACCM material will be portion marked with the appropriate classification level abbreviation (e.g. (S)), “ACCM,” and the program’s nickname. Use a hyphen (-) without interjected spaces to separate the “ACCM” caveat and the program’s nickname. Separate multiple nicknames with a single forward slash (/).

(4) The portion mark “ACCM” may be used when the applicable programs are the same as the programs listed in the banner line. If the applicable programs are different than shown in the banner line, the complete portion marking must be used (see Figure 59).

(5) Only the full nickname may be used after the “ACCM” caveat. No abbreviations or derivations (e.g., digraph or trigraph) of the nickname may be used in place of the full nickname in the banner line or portion markings of ACCM-protected information.

b. Department of State (DoS) Dissemination Control Markings. DoS dissemination control markings are provided, for information, in Appendix 3 to this enclosure. Such markings may not be applied in the first instance by DoD personnel.

c. Equivalent Foreign Security Classifications. Current equivalent foreign security classifications will be listed and available for reference at the OUSD(P) SIPRNET website <https://intelshare.intelink.sgov.gov/sites/isp/default.aspx>.

Appendixes

1. Dissemination Control Markings for Intelligence Information
2. DoS Dissemination Control Markings

APPENDIX 1 TO ENCLOSURE 4

DISSEMINATION CONTROL MARKINGS FOR INTELLIGENCE INFORMATION

1. CONTROLLED IMAGERY (IMCON)

a. IMCON is used to protect sources and analytic methods associated with the geospatial intelligence discipline that are particularly vulnerable to countermeasures, and if disclosed or released could negate or measurably reduce the effectiveness of those methodologies.

b. IMCON may be applied ONLY to information classified at the SECRET level.

c. Imagery and/or text reporting bearing the IMCON marking requires a dissemination notice to be applied. See Reference (o) for details.

d. For additional information on proper markings, control and releasability of IMCON, refer to References (m) and (am), the NGA Security Classification Guide, and the sensitive analytical techniques Web page, or contact the NGA Disclosure Office.

e. The IMCON material must be classified SECRET (see Figure 54); however, if IMCON information is included in a paragraph containing TOP SECRET information, the appropriate classification would be TOP SECRET//IMCON.

f. The banner line of documents containing both IMCON and NOFORN portions must be marked //IMCON/NOFORN, with a classification no lower than SECRET (see Figure 55).

g. IMCON information may not be processed on SIPRNET without prior approval from the Sensitive Analytical Techniques Panel. Contact the panel chair for additional information.

Figure 55. Example of IMCON Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

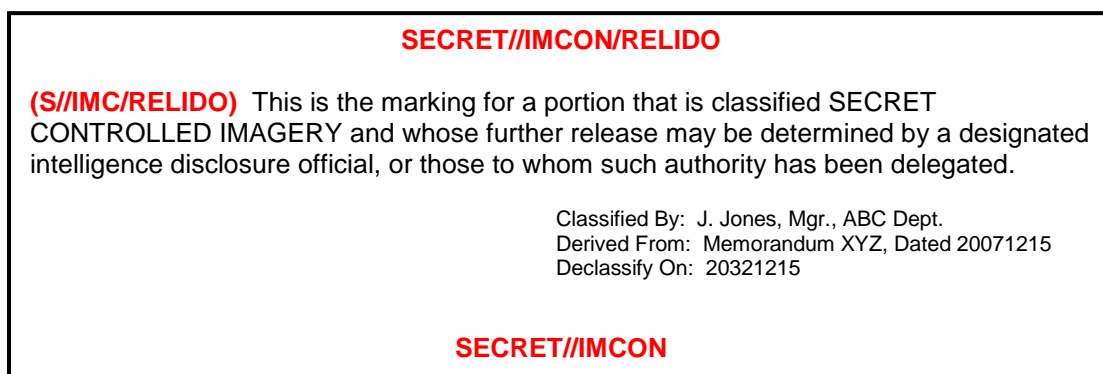
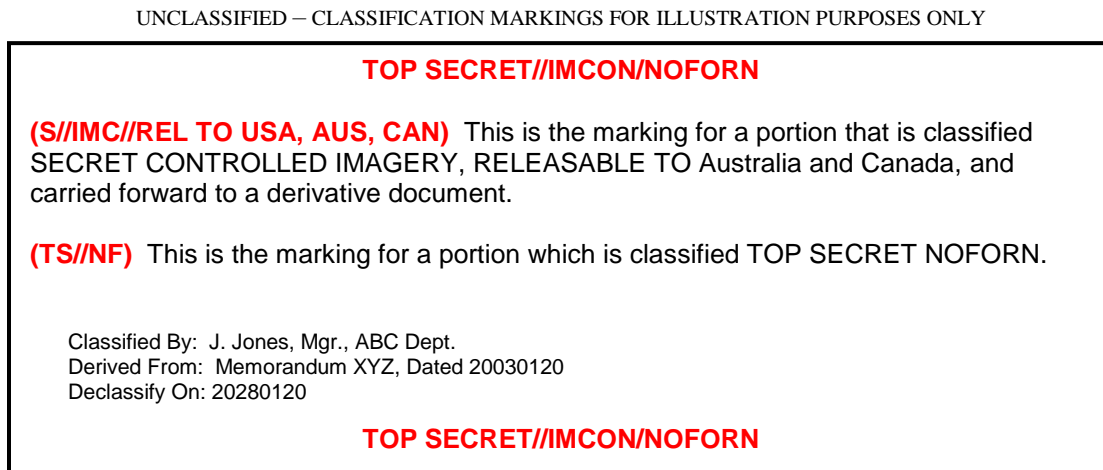


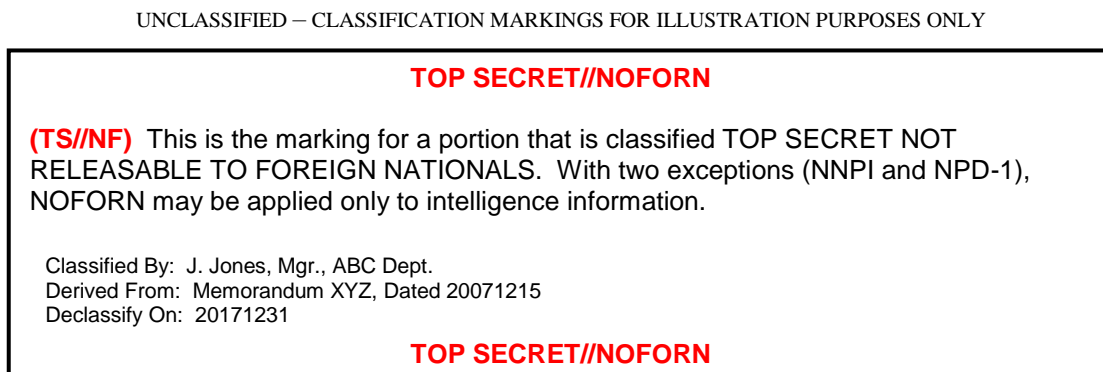
Figure 56. Example of IMCON Banner Marking When There Are NOFORN Portions



2. NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN)

a. NOFORN is applied, in accordance with section XI.E of Reference (am), to classified intelligence that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens without permission of the originator of the information (see Figure 56).

Figure 57. Example of NOFORN Marking



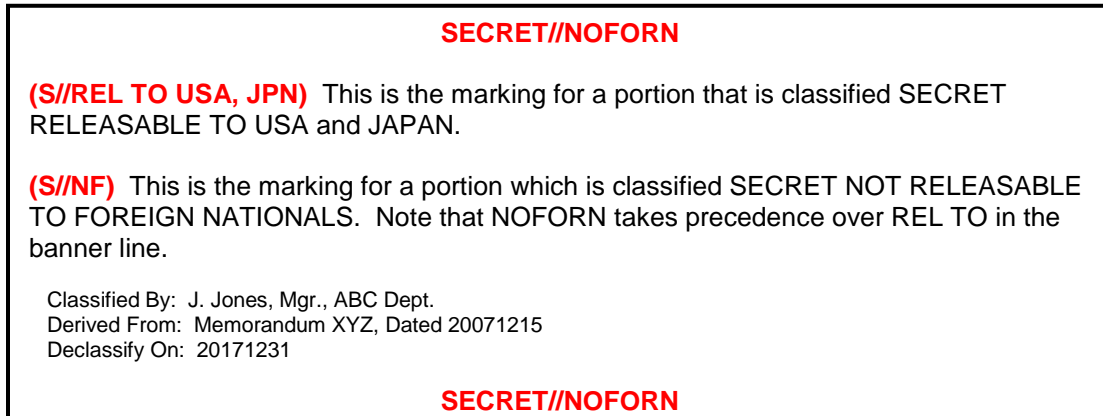
b. NOFORN shall NOT be applied to non-intelligence information, except for NNPI, NDP-1, and cover and cover support information in accordance with Reference (y), which have authorized exceptions for use of NOFORN. In all other instances, within the DoD NOFORN shall be used ONLY on intelligence information.

c. NOFORN may be used only with TOP SECRET, SECRET, CONFIDENTIAL, or CUI.

d. It cannot be used with REL TO or RELIDO in the banner line. When a document contains NOFORN and REL TO or NOFORN and RELIDO portions, NOFORN takes precedence for the markings in the banner line (see Figure 57).

Figure 58. Example of NOFORN Markings with REL TO Portions

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



e. All national intelligence, which is under the purview of the DNI, is to be explicitly marked at both the banner and portion level for foreign disclosure or release in accordance with Reference (m)). However, Reference (m) is not applicable to classified military intelligence subject to disclosure or release under NDP-1. The NOFORN caveat should be used as infrequently as possible on otherwise uncaveated classified military intelligence. Absence of the NOFORN caveat allows foreign disclosure officials to exercise their discretionary authority in accordance with References (x), (am), and (ao).

3. PROPRIETARY INFORMATION INVOLVED (PROPIN)

a. PROPIN is a control marking used by the IC to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value (see Figure 58). The marking may not be used on DoD documents except where those documents use IC information so marked. The marking may be used on U.S. Government proprietary information (e.g., budget or financial information) ONLY when that information can provide an unfair advantage (e.g., for contractor(s)).

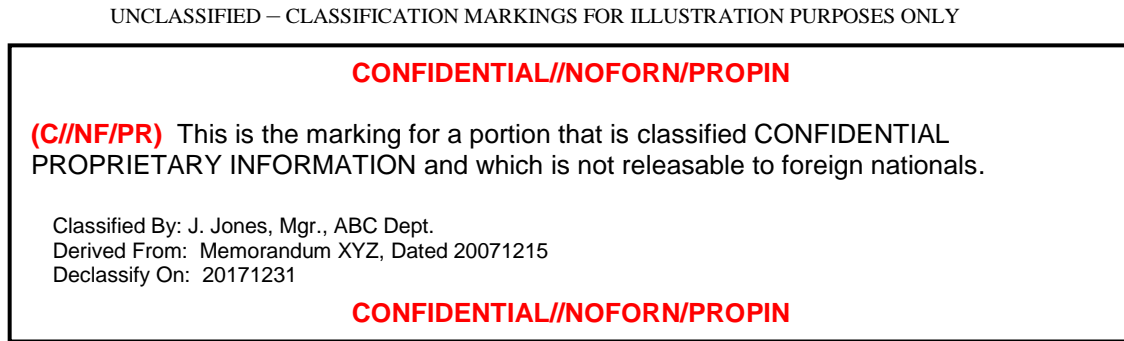
b. PROPIN may be used with TOP SECRET, SECRET, CONFIDENTIAL, or UNCLASSIFIED.

c. PROPIN appears in the banner if any portion contains PROPIN information.

d. Information marked as PROPIN may not be disseminated outside the Federal Government in any form without the express permission of the originator and the provider of the proprietary information.

e. The PROPIN control marking precludes dissemination to contractors irrespective of their status to, or within, the U.S. Government without the authorization of the originator and the provider of the information.

Figure 59. Example of PROPIN Marking



4. RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL (RELIDO)

a. RELIDO is a dissemination control marking that may be applied to national intelligence information to indicate that the originator has authorized Designated Intelligence Disclosure Officials (DIDOs), or their designee, to make further release determinations in accordance with existing foreign disclosure policy and procedures (see Figure 59). (See References (m) and (ao) for further information.)

b. RELIDO may be used only with national intelligence information.

c. RELIDO may be used only with TOP SECRET, SECRET, or CONFIDENTIAL. It may be used independently or with REL TO.

d. RELIDO may not be used in the same portion or banner line with NOFORN. When a document contains both NOFORN and RELIDO portions, NOFORN takes precedence for the markings in the banner line.

e. Only DIDOs, or their designees, are authorized to further release information marked RELIDO without consulting the originator. Defense Intelligence Component Foreign Disclosure Officers (FDO) are not authorized to release information marked RELIDO unless specifically authorized. DIDOs may sub-delegate this authority, in writing, to FDOs within their organizations who have received formal training on disclosure and release of national intelligence and use of the RELIDO marking, and whose responsibilities include making release decisions for national intelligence produced by their organizations. Contact the local foreign disclosure office for further guidance on RELIDO processes and procedures. Check the CAPCO website for a list of DIDOs.

Figure 60. Example of RELIDO Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

SECRET//RELIDO

(S//RELIDO) This is the marking for a portion that is classified SECRET which the originator has determined is RELEASABLE BY INFORMATION DISCLOSURE OFFICIAL. This marking explicitly states that a DIDO, or designee(s), may release the material in accordance with existing foreign disclosure policy and procedures.

(S//REL TO USA, AUS, CAN/RELIDO) This is the marking for a portion that is classified SECRET in which the originator has made a release decision for the listed countries. RELIDO allows a DIDO, or designee(s), to make the decision to further release the information to other countries.

(U) The RELIDO marking is carried in the banner line because it is stated in all portions.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171231

SECRET//RELIDO

5. FISA

a. The FISA control marking denotes the presence of FISA or FISA-derived information in the document. This is an informational marking only to highlight such information. The FISA control marking required by this Volume does not satisfy or alter the legal requirement for such information to be accompanied by the FISA warning or caveat described in subparagraph 5.b. of this section.

b. In accordance with section 1801, et. seq., of title 50, U.S.C (also known as the Foreign Intelligence Surveillance Act of 1978, as amended (Reference (aq))), information collected pursuant to the statute may not be disclosed for law enforcement purposes unless the disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with advance authorization of the Attorney General of the United States.

c. Specific wording of the applicable FISA warning or caveat must be provided by the cognizant legal office (see Figure 60). The FISA warning or caveat should be collocated with the FISA or FISA-derived information; however, when necessary due to formatting limitations of some electronic systems, the FISA warning or caveat may appear at the top or bottom (e.g., in the header or footer) of the document.

d. Both the banner and portion marking use the abbreviation FISA.

Figure 61. Example of FISA Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

TOP SECRET//NOFORN/FISA

Applicable FISA Warning or Caveat (contact the cognizant legal office for wording of the required warning or caveat.)

(TS//NF/FISA) This is the marking for a portion which is TOP SECRET, is not releasable to foreign nationals, and contains FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) information.

Classified By: J. Jones, Mgr., ABC Dept.
Derived From: Memorandum XYZ, Dated 20071215
Declassify On: 20171215

TOP SECRET//NOFORN/FISA

APPENDIX 2 TO ENCLOSURE 4

DOS DISSEMINATION CONTROL MARKINGS

1. EXCLUSIVE DISTRIBUTION (EXDIS)

a. EXDIS is a DoS marking used with classified information or CUI (see Figure 67). The portion marking for EXDIS information is ([classification]//XD).

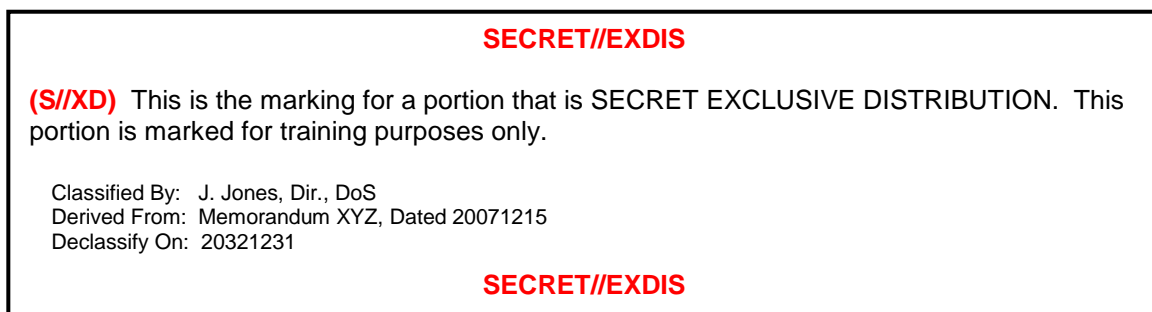
b. This distribution control is used only for highly sensitive message traffic sent among the President; the Secretary, Deputy Secretary, or Under Secretaries of State; and the DoS Chiefs of Mission.

c. Documents bearing this marking may not be released to foreign governments or international organizations.

d. EXDIS and no distribution (NODIS) markings may not be used together. Only one or the other shall be used on a document.

Figure 62. Example of EXDIS Marking

UNCLASSIFIED – CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY



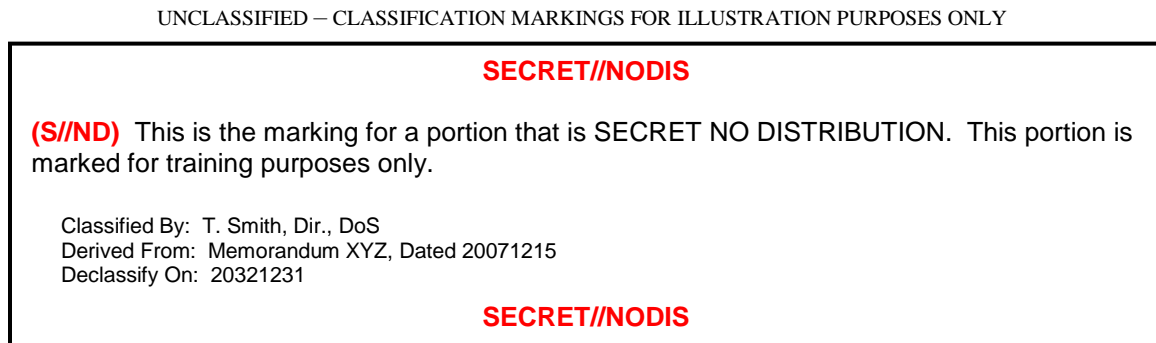
2. NODIS

a. NODIS is a DoS marking used only on messages of the highest sensitivity among the President, the Secretary of State, and a DoS Chief of Mission. It may be used with classified information or CUI. The portion marking for NODIS is ([classification]//ND) (see Figure 62).

b. NODIS messages are “eyes-only,” to be read only by individuals named in the distribution instructions or by those designated to receive NODIS. Such messages may not be shown to anyone other than the addressees, even if the named individuals determine that those under their authority have a need to know, without prior approval from the DoS Operations Center. If more than one official has been authorized to see NODIS material, maintain an official record of every individual who reads each incoming message.

- c. Information contained in NODIS messages may not be reproduced or used in other products without prior approval from the DoS Operations Center. Do NOT photocopy or forward NODIS messages electronically.
- d. Documents bearing this distribution control shall be administratively controlled as NOFORN and may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-US citizens.
- e. NODIS and EXDIS markings may not be used together. Only one or the other may be used on a portion.
- f. NODIS has priority over EXDIS in the banner line.

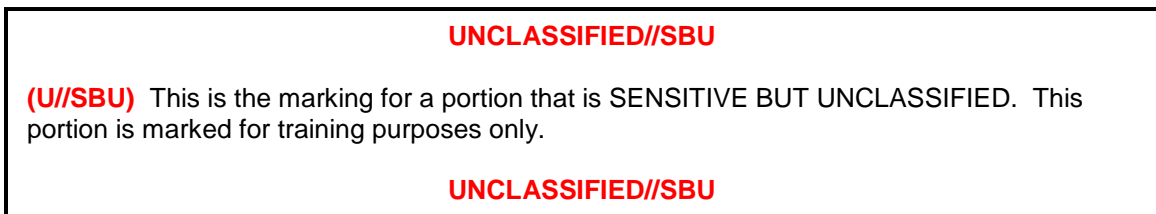
Figure 63. Example of NODIS Marking



3. SENSITIVE BUT UNCLASSIFIED (SBU)

- a. SBU is a DoS marking used on unclassified information (see Figure 63), originated within DoS, that warrants a degree of protection and administrative control and meets criteria for exemption from mandatory public disclosure under the Freedom of Information Act.
- b. SBU shall be used only derivatively within the DoD.
- c. Volume 4 of this Manual provides guidance on the use of SBU.

Figure 64. Example of SBU Marking



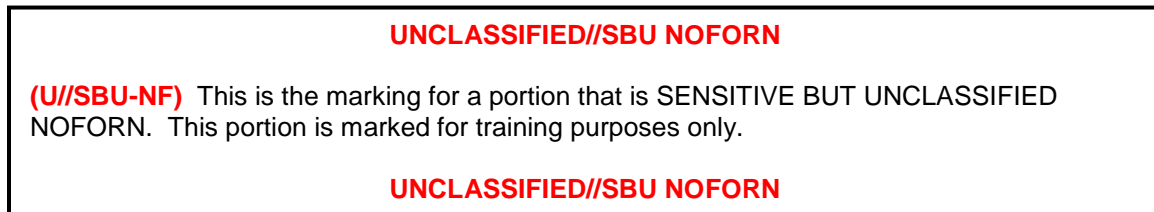
4. SENSITIVE BUT UNCLASSIFIED-NOFORN (SBU-NF)

a. SBU-NF is a marking for unclassified information originated within the DoS that warrants a degree of protection and administrative control, meets criteria for exemption from mandatory public disclosure under the Freedom of Information Act, and is prohibited from dissemination to non-U.S. citizens (see Figure 64).

b. This marking is used only with UNCLASSIFIED information. It shall only be used derivatively within the DoD. See Volume 4, Enclosure 3 of this Manual for further guidance regarding use of SBU-NF information.

c. As this is a DoS marking, this use of NOFORN falls outside the DoD policy guidance which permits use of NOFORN only on classified intelligence information, NNPI, NDP-1, and cover and cover support information in accordance with Reference (y).

Figure 65. Example of SBU-NF Marking



GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ACCM	alternative compensatory control measures
AEA	Atomic Energy Act
C	Confidential
CAPCO	Controlled Access Program Coordination Office
CDO	controlling DoD office
CNWDI	Critical Nuclear Weapon Design Information
CTS	COSMIC Top Secret
CUI	controlled unclassified information
DCID	Director of Central Intelligence Directive
DDI(CL&S)	Director of Defense Intelligence (Counterintelligence, Law Enforcement, & Security)
DEA	Drug Enforcement Administration
DIDO	Designated Intelligence Disclosure Official
DNI	Director of National Intelligence
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DOE	Department of Energy
DoS	Department of State
DTM	Directive-Type Memorandum
DVD	digital video disc (also digital versatile disc)
E.O.	Executive Order
EXDIS	Exclusive Distribution
FDO	Foreign Disclosure Officer
FGI	foreign government information
FISA	Foreign Intelligence Surveillance Act
FOUO	For Official Use Only
FRD	Formerly Restricted Data
FSE	file series exemption
G	Gamma
HCS	HUMINT Control System
HUMINT	human intelligence
HVSACO	Handle via Special Access Channels Only
IAW	in accordance with

IC	Intelligence Community
ICD	Intelligence Community Directive
IT	information technology
IMCON	Controlled Imagery
ISCAP	Interagency Security Classification Appeals Panel
ISO	International Organization for Standardization
ISOO	Information Security Oversight Office
IT	information technology
JWICS	Joint Worldwide Intelligence Communications System
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NDP	National Disclosure Policy
NF	NOFORN
NGA	National Geospatial-Intelligence Agency
NNPI	Naval Nuclear Propulsion Information
NODIS	No Distribution
NOFORN	not releasable to foreign nationals
NC	NATO Confidential
NR	NATO Restricted
NS	NATO Secret
NSI	national security information
NU	NATO Unclassified
OADR	originating agency's determination required
OCA	original classification authority
ODNI	Office of the Director of National Intelligence
ORCON	originator controlled
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
POC	point of contact
PROPIN	proprietary information
RD	Restricted Data
RELIDO	releasable by Information Disclosure Official
REL TO	authorized for release to
S	Secret
SAMI	Sources and Methods Information
SAP	Special Access Program
SBU	sensitive but unclassified
SBU-NF	sensitive but unclassified-NOFORN
SCI	Sensitive Compartmented Information
SF	Standard Form
SI	Special Intelligence

SIGINT	signals intelligence
SIPRNET	Secret Internet Protocol Router Network
SNM	special nuclear material
TK	Talent Keyhole
TS	Top Secret
U	Unclassified
UCNI	Unclassified Controlled Nuclear Information
U.S.C.	United States Code
URL	uniform resource locator
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Volume.

ATOMAL. Applies to U.S. RD or FRD, or UK ATOMIC information that has been officially released to NATO.

CDO. The DoD activity that sponsored the work that generated the technical data or received the technical data on behalf of the DoD and, therefore, has the responsibility for determining the distribution of a document containing such technical data. For joint sponsorship, the controlling office is determined by advance agreement and may be a party, group, or committee representing the interested activities or the DoD Components.

classified national security information. Information that has been determined pursuant to Reference (d), or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

CNWDI. A DoD designation for TOP SECRET or SECRET RD weapon data revealing the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munitions, or test device.

collateral information. Information identified as classified national security information which is not subject to the enhanced security protections (e.g., safeguarding, access requirements) required for SCI or SAP information.

COSMIC. TOP SECRET material that belongs to NATO.

date of original classification. The date a document is determined to be classified. For example, classification would begin from the date a document is created, not from the date of any security classification guide used to authorize classification of that document.

defense articles. For purposes of the Defense Trade Cooperation Treaty between the United States and Australia or the United Kingdom, those articles, services, and related technical data, including software, in tangible or intangible form, listed on the United States Munitions List of

the International Traffic in Arms Regulations (ITAR) (Reference (at)), as modified or amended. Defense articles exempt from the scope of section 126.17 of the Reference (at) are identified in Supplement No. 1 to Part 126 of Reference (at).

Defense Intelligence Components. All DoD organizations that perform national intelligence, Defense Intelligence, and intelligence-related functions, including: the Defense Intelligence Agency; the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency/Central Security Service, and the intelligence elements of the Active and Reserve components of the Military Departments, including the United States Coast Guard when operating as a service in the Navy.

Defense Purpose Rights. The legal rights established by international agreement that authorizes the U.S. DoD to have full data rights to information.

derivative classification. The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

dissemination control markings. Markings that identify the expansion or limitation on the distribution of information.

distribution statement. A statement used on a technical document to denote the extent of its availability for secondary distribution, release, and disclosure without additional approvals or authorizations. A distribution statement is distinct from and in addition to a security classification marking and any dissemination control markings included in the banner line. A distribution statement is also required on security classification guides submitted to DTIC.

document face. The first page, title page or front cover of the document

element of the Intelligence Community. See Intelligence Community.

FGI. 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.

Information produced by the U.S. Government pursuant to or as a result of an arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence and to which the U.S. Government does not have Defense Purpose Rights.

Information received and treated as “Foreign Government Information” pursuant to the terms of a predecessor order to Reference (d).

file series exemption. An exception to the 25-year automatic declassification provisions of Reference (d). This exception applies to entire blocks of records, i.e., “file series,” within an agency’s records management program. To qualify for this exemption, the file series must be replete with exemptible information.

foreground information. Classified or unclassified information developed as part of an International Cooperative Program to which the U.S. DoD has Defense Purpose Rights.

FOUO. A protective marking to be applied to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more provisions of the Freedom of Information Act. This includes information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended. See DoD 5400.7-R (Reference (al)) for detailed information on categories of information that may qualify for exemption from public disclosure. The use of FOUO marking remains in effect until the implementation of the CUI DoDI.

FRD. Information removed from the RD category upon a joint determination by the Departments of Energy and Defense that such information relates primarily to the military utilization of atomic weapons.

information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

Intelligence Community. An element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of E.O. 12333 (Reference (as)).

Joint information. Information owned or produced by more than one country or international organization. Foreground information developed as a part of an international cooperative program to which the U.S. has co-ownership and/or Defense Purpose Rights. Classified foreign government information to which the U.S. has Defense Purpose Rights, regardless of whether U.S. classified information is shared with the foreign partner.

need to know. A determination within the Executive Branch that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

NSI. Information that has been determined, pursuant to Reference (d), or any predecessor order, to require protection against unauthorized disclosure.

OCA. An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information (i.e., to classify information in the first instance).

original classification. An original determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

page marking. Banner marking at top and/or bottom of an interior page of a document.

RD. All data concerning design, manufacture, or utilization of nuclear weapons; the production of SNM; and the use of SNM for production of energy, but not data declassified or removed from the RD category pursuant to section 2162 of The Atomic Energy Act of 1954, as amended.

SAP. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. In the DoD, any DoD program or activity (as authorized in Reference (d)), employing enhanced security measures (e.g., safeguarding, access requirements), exceeding those normally required for collateral information at the same level of classification, shall be established, approved, and managed as a DoD SAP in accordance with Reference (ae).

SCI. Classified national intelligence information concerning, or derived from, intelligence sources, methods or analytical processes that requires handling within formal access control systems established by the DNI.

Sigma 14 information. The subcategory of RD and FRD consisting of sensitive information (including bypass scenarios) concerning the vulnerability of nuclear weapons to a deliberate unauthorized nuclear detonation.

SNM. Defined in Reference (ak).

source document. An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

tetragraph. A sequence of four letters used to represent an international organization, alliance or other grouping of countries and international organizations.

trigraph. A sequence of three letters used to represent a country. Also called country code.

unauthorized disclosure. Communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient.

wiki. A collaborative website that allows users to modify previously posted content by adding, deleting or editing the information.

weapons of mass destruction. Any weapon of mass destruction as defined in section 1801(p) of Reference (aq).

working paper. Documents and material accumulated or created in the preparation of finished documents and material.



Department of Defense MANUAL

NUMBER 5200.01, Volume 3
February 24, 2012
Incorporating Change 2, March 19, 2013

USD(I)

SUBJECT: DoD Information Security Program: Protection of Classified Information

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP). This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526, E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (CFR) (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume:

- (1) Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information.
- (2) Identifies security education and training requirements and processes for handling of security violations and compromise of classified information.
- (3) Addresses information technology (IT) issues of which the security manager must be aware.
- (4) Incorporates and cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandums (References (g) and (h)).

2. APPLICABILITY. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereinafter referred to collectively as the “DoD Components”).

b. Does not alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community pursuant to policies issued by the DNI. Consistent with Reference (b), SCI shall be safeguarded in accordance with the policies and procedures issued by the DNI, as implemented by DoD 5105.21-M-1 (Reference (i)) and other applicable guidance.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy, in accordance with Reference (b), to:

a. Identify and protect national security information and CUI in accordance with national-level policy issuances.

b. Promote information sharing, facilitate judicious use of resources, and simplify management through implementation of uniform and standardized processes.

c. Employ, maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting classified information.

d. Actively promote and implement security education and training throughout the Department of Defense.

e. Mitigate the adverse effects of unauthorized access to classified information by investigating and acting upon reports of security violations and compromises of classified information.

5. RESPONSIBILITIES. See Enclosure 2 of Volume 1.

6. PROCEDURES. See Enclosures 2 through 7.


7. INFORMATION COLLECTION REQUIREMENTS. All inspections, investigations, notifications, and audits required by this Volume are exempt from licensing according to paragraphs C4.4.1, C4.4.2, C4.4.7 and C4.4.8 of DoD 8910.1-M (Reference (j)).

8. RELEASABILITY. UNLIMITED. This Volume is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

9. EFFECTIVE DATE. This Volume:

a. Is effective February 24, 2012.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (ck)). If not, it will expire effective February 24, 2022 and be removed from the DoD Issuances Website.



Michael G. Vickers
Under Secretary of Defense
for Intelligence

Enclosures

1. References
2. Safeguarding
3. Storage and Destruction
4. Transmission and Transportation
5. Security Education and Training
6. Security Incidents Involving Classified Information
7. IT Issues for the Security Manager

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....9

ENCLOSURE 2: SAFEGUARDING.....14

 CONTROL MEASURES14

 PERSONAL RESPONSIBILITY FOR SAFEGUARDING14

 ACCESS TO CLASSIFIED INFORMATION14

 DETERMINING NEED FOR ACCESS14

 EMERGENCY AUTHORITY14

 ACCESS BY INDIVIDUALS OUTSIDE THE EXECUTIVE BRANCH.....15

 Congress.....16

 Government Printing Office (GPO).....16

 Representatives of the Government Accountability Office (GAO).....16

 Historical Researchers16

 Presidential or Vice Presidential Appointees and Designees18

 Use of Classified Information in Litigation.....18

 Special Cases18

 VISITS18

 PROTECTION WHEN REMOVED FROM STORAGE.....19

 END OF DAY SECURITY CHECKS19

 EMERGENCY PLANS19

 USE OF SECURE COMMUNICATIONS20

 REMOVAL OF CLASSIFIED INFORMATION FOR WORK AT HOME.....20

 Top Secret.....20

 Secret and Confidential.....20

 Residential Storage Equipment.....20

 Classified IT Systems20

 Foreign Country Restriction20

 WORKING PAPERS.....21

 EQUIPMENT USED FOR PROCESSING CLASSIFIED INFORMATION21

 REPRODUCTION OF CLASSIFIED MATERIAL22

 CLASSIFIED MEETINGS AND CONFERENCES.....23

 SAFEGUARDING FGI.....26

 North Atlantic Treaty Organization (NATO) Information.....26

 Other FGI.....26

 ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM)29

 DoD Proponents for ACCM29

 ACCM Approval.....29

 Guidance on ACCM Use29

 Prohibited Security Measures30

 Prohibited Uses of ACCM30

 Documentation.....31

 Annual Reports of ACCM Use31

Sharing ACCM-Protected Information.....31
Contractor Access to ACCM32
Program Maintenance32
Safeguarding ACCM Information32
Security Incidents.....33
ACCM Termination34
Transitioning an ACCM to a SAP34

ENCLOSURE 3: STORAGE AND DESTRUCTION35

GENERAL REQUIREMENTS35
LOCK SPECIFICATIONS35
STORAGE OF CLASSIFIED INFORMATION BY LEVEL OF CLASSIFICATION.....35
 Top Secret35
 Secret.....36
 Confidential.....37
RISK ASSESSMENT37
U.S. CLASSIFIED INFORMATION LOCATED IN FOREIGN COUNTRIES37
SPECIALIZED STORAGE.....38
 Military Platforms38
 IT Equipment38
 Map and Plan File Cabinets38
 Modular Vaults38
 Bulky Material38
PROCURING NEW STORAGE EQUIPMENT39
SECURITY CONTAINER LABELS39
EXTERNAL MARKINGS ON CONTAINERS39
SECURITY CONTAINER INFORMATION39
COMBINATIONS TO CONTAINERS, VAULTS AND SECURE ROOMS40
 Protecting and Storing Combinations40
 Changing Combinations.....40
ENTRANCES TO OPEN STORAGE AREAS FOR CLASSIFIED INFORMATION41
INSPECTION OF STORAGE CONTAINERS PRIOR TO REMOVAL, REPAIR, ETC.....41
NEUTRALIZATION AND REPAIR PROCEDURES41
STORAGE OF FGI.....41
RETENTION OF CLASSIFIED INFORMATION42
DESTRUCTION OF CLASSIFIED INFORMATION42
TECHNICAL GUIDANCE ON DESTRUCTION METHODS43
 Crosscut Shredders.....43
 Pulverizers and Disintegrators44
 Pulping44
DESTRUCTION PROCEDURES44

APPENDIX:
PHYSICAL SECURITY STANDARDS45

ENCLOSURE 4: TRANSMISSION AND TRANSPORTATION.....53

- TRANSMISSION AND TRANSPORTATION PROCEDURES.....53
- DISSEMINATION OUTSIDE THE DEPARTMENT OF DEFENSE.....53
- TRANSMISSION OF TOP SECRET INFORMATION54
- TRANSMISSION OF SECRET INFORMATION55
- TRANSMISSION OF CONFIDENTIAL INFORMATION.....57
- TRANSMISSION OF CLASSIFIED INFORMATION AND MATERIAL TO FOREIGN GOVERNMENTS57
- SECURITY REQUIREMENTS FOR TRANSFERS OF DEFENSE ARTICLES TO AUSTRALIA AND THE UNITED KINGDOM WITHOUT AN EXPORT LICENSE OR OTHER WRITTEN AUTHORIZATION.....58
 - Background.....58
 - Applicability58
 - Marking.....59
 - Transfer.....60
- USE OF SECURE COMMUNICATIONS FOR TRANSMISSION OF CLASSIFIED INFORMATION60
 - Computer-To-Computer Transmission.....60
 - Facsimile (Fax) Transmission.....61
 - Telephone.....61
- SHIPMENT OF BULK CLASSIFIED MATERIAL AS FREIGHT61
- PREPARATION OF MATERIAL FOR SHIPMENT61
- USE OF BRIEFCASES OR ZIPPERED POUCHES FOR HAND-CARRYING CLASSIFIED MATERIAL62
- ESCORT, COURIER, OR HAND-CARRY OF CLASSIFIED MATERIAL.....63
 - Authority.....63
 - Packaging Requirements.....64
 - Responsibilities.....64
 - Customs, Police and Immigration.....64
 - Disclosure Authorization65
- ESCORT, COURIER, OR HAND-CARRY AUTHORIZATION.....65
- HAND-CARRYING OR ESCORTING CLASSIFIED INFORMATION ON COMMERCIAL AIRCRAFT.....66

APPENDIX:

- TRANSFER OF CLASSIFIED INFORMATION OR MATERIAL TO FOREIGN GOVERNMENTS68

ENCLOSURE 5: SECURITY EDUCATION AND TRAINING75

- REQUIREMENT.....75
- SECURITY EDUCATION AND TRAINING RESOURCES.....75
- INITIAL ORIENTATION.....75
- SPECIAL TRAINING REQUIREMENTS78
- OCA TRAINING.....79

DECLASSIFICATION AUTHORITY TRAINING82
ANNUAL REFRESHER TRAINING.....82
CONTINUING SECURITY EDUCATION AND TRAINING.....83
TERMINATION BRIEFINGS84
MANAGEMENT AND OVERSIGHT TRAINING84
PROGRAM OVERSIGHT85

ENCLOSURE 6: SECURITY INCIDENTS INVOLVING CLASSIFIED INFORMATION ...86

INTRODUCTION86
CONSEQUENCES OF COMPROMISE87
REPORTING AND NOTIFICATIONS87
CLASSIFICATION OF REPORTS89
SPECIAL CIRCUMSTANCES.....89
 Security Incidents Involving Deliberate Compromise, a Foreign Intelligence Service
 or a Terrorist Organization.....89
 Security Incidents Involving Apparent Violations of Criminal Law90
 Security Incidents Involving COMSEC or Cryptologic Information90
 Security Incidents Involving SCI.....90
 Security Incidents Involving RD and/or FRD90
 Security Incidents Involving IT90
 Security Incidents Involving FGI or NATO Information90
 Security Incidents Involving Classified U.S. Information Provided to Foreign
 Governments91
 Security Incidents Involving SAPs91
 Security Incidents Involving Improper Transfer of Classified Information91
 Security Incidents Involving On-Site Contractors91
 Security Incidents Involving Critical Program Information (CPI)91
 Security Incidents Involving ACCM-Protected Information.....92
 Absence Without Authorization92
 Coordination with Legal Counsel and the Department of Justice (DoJ)92
SECURITY INQUIRIES AND INVESTIGATIONS92
 Requirement92
 Coordination with Criminal Investigative Organization or Defense CI Component92
 Coordination with OCA93
 Security Inquiries93
 Security Investigations.....94
INFORMATION APPEARING IN THE PUBLIC MEDIA95
RESULTS OF INQUIRIES AND INVESTIGATIONS96
ACTIONS TO BE TAKEN BY THE OCA97
DAMAGE ASSESSMENTS98
VERIFICATION, REEVALUATION, AND DAMAGE ASSESSMENT TIME LINES.....99
ACTUAL OR POTENTIAL COMPROMISES INVOLVING MORE THAN ONE
 AGENCY99
DEBRIEFING IN CASES OF UNAUTHORIZED ACCESS99
REPORTING AND OVERSIGHT MECHANISMS100

APPENDIXES

- 1. SECURITY INCIDENT REPORTING FORMAT101
- 2. DOJ MEDIA LEAK QUESTIONNAIRE103

ENCLOSURE 7: IT ISSUES FOR THE SECURITY MANAGER104

- OVERVIEW104
- RESPONSIBILITY.....104
- IA ROLES AND FUNCTIONS.....104
- IA CONCEPTS.....104
 - IA Attributes105
 - System Categorization105
 - Certification and Accreditation (C&A)105
- DATA SPILLS.....106
- DISPOSAL OF COMPUTER MEDIA108
- NON-TRADITIONAL WORK ENVIRONMENTS.....108
- REQUIREMENT FOR ENCRYPTION OF CERTAIN UNCLASSIFIED DATA.....109
- PII.....109
- NEW TECHNOLOGY AND EQUIPMENT109
- INTERNET-BASED SOCIAL NETWORKING SERVICES110
- MARKING REQUIREMENTS FOR ELECTRONIC INFORMATION.....110
- PROCESSING REQUIREMENTS FOR SPECIFIC TYPES OF INFORMATION110
 - SCI110
 - RD and Critical Nuclear Weapons Design Information (CNWDI).....111
 - SAP111
 - Controlled Imagery111
 - NATO Information111
 - CUI.....111
- COMPILATION AND DATA AGGREGATION111

GLOSSARY112

- PART I. ABBREVIATIONS AND ACRONYMS112
- PART II. DEFINITIONS.....114

FIGURES

- 1. Conditions Governing Access to Official Records for Research Historical Purposes17
- 2. Report of Security Incident Inquiry or Investigation.....102

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (b) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive
Compartmented Information," October 9, 2008
- (c) DoD 5200.1-R, "Information Security Program," January 14, 1997 (cancelled by Volume 1
of this Manual)
- (d) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (e) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
- (f) Part 2001 of title 32, Code of Federal Regulations
- (g) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
Memorandum, "Revised Alternative Compensatory Control Measures (ACCM) Guidance,"
April 18, 2003 (hereby cancelled)
- (h) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
Memorandum, "Classified Information at Meetings and Conferences," October 26, 2001
(hereby cancelled)
- (i) DoD 5105.21-M-1, "Department of Defense Sensitive Compartmented Information
Administrative Security Manual," August 1998
- (j) DoD 8910.1-M, "Department of Defense Procedures for Management of Information
Requirements," June 30, 1998
- (k) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22,
2008
- (l) DoD 5200.2-R, "Personnel Security Program," January 1, 1987
- (m) DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
- (n) Department of Defense/Government Printing Office Security Agreement, 1981¹
- (o) DoD Instruction 7650.01, "Government Accountability Office (GAO) and Comptroller
General Requests for Access to Records," January 27, 2009
- (p) DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony by
DoD Personnel as Witnesses," July 23, 1985
- (q) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (r) Committee on National Security Systems Instruction 4004, "Destruction and Emergency
Protection Procedures for COMSEC and Classified Material," August 2006²
- (s) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation
Process (DIACAP)," November 28, 2007
- (t) Chapters 22 and 33 of title 44, United States Code
- (u) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
- (v) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (w) DoD Directive C-5200.19, "Control of Compromising Emanations (U)," May 16, 1995

¹ Contact Security Directorate, Office of the Deputy Under Secretary of Defense for Intelligence

² Documents issued by the Committee on National Security Systems (CNSS) are available at www.cnss.gov/full-index.html

- (x) DoD 5220.22-M, “National Industrial Security Program Operating Manual,” February 28, 2006
- (y) Parts 120 through 130 of title 22, Code of Federal Regulations (also known as “The International Traffic in Arms Regulations”)
- (z) DoD Directive 5230.11, “Disclosure of Classified Military Information to Foreign Governments and International Organizations,” June 16, 1992
- (aa) DoD Instruction 2000.16, “DoD Antiterrorism (AT) Standards,” October 2, 2006
- (ab) DoD Instruction 5240.05, “Technical Surveillance Countermeasures (TSCM) Program,” February 22, 2006
- (ac) United States Security Authority for NATO Affairs Instruction 1-07, “Implementation of NATO Security Requirements,” April 5, 2007³
- (ad) Department of Defense and United Kingdom Ministry of Defense, “Security Implementing Arrangement,” January 27, 2003⁴
- (ae) Chairman of the Joint Chiefs of Staff Manual 3150.29C, “Code Word, Nickname, and Exercise Terms Report (NICKA) System,” December 7, 2007⁵
- (af) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003
- (ag) Chairman of the Joint Chiefs of Staff Manual 5720.01B, “Joint Staff Message Management and Preparation,” February 15, 2005⁶
- (ah) DoD Directive 5205.07, “Special Access Program (SAP) Policy,” July 1, 2010
- (ai) DoD Directive 5210.56, “Carrying of Firearms and the Use of Force by DoD Personnel Engaged in Security, Law and Order, or Counterintelligence Activities,” April 1, 2011
- (aj) DoD Instruction 3224.03, “Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E),” October 1, 2007
- (ak) Federal Specification FF-L-2740, “Locks, Combination,” current edition⁷
- (al) Federal Standard 832, “Construction Methods and Materials for Vaults,” September 1, 2002⁷
- (am) Federal Specification FF-L-2937, “Combination Lock, Mechanical,” January 31, 2005, as amended⁷
- (an) Federal Specification AA-F-358, “Filing Cabinet, Legal and Letter Size, Uninsulated, Security,” current edition⁸
- (ao) Federal Specification AA-V-2737, “Modular Vault Systems,” April 25, 1990, with Amendment 2, October 30, 2006⁷
- (ap) Federal Specification FF-P-110, “Padlock, Changeable Combination (Resistant To Opening By Manipulation and Surreptitious Attack),” current edition, as amended⁷
- (aq) Section 1386 of title 18, United States Code
- (ar) Federal Standard 809, “Neutralization and Repair of GSA Approved Containers and Vault Doors,” current edition⁷

³ Available to authorized recipients from the Central U.S. Registry

⁴ Contact the Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy

⁵ Restricted distribution. Contact J-3, Office of the Joint Chiefs of Staff

⁶ This document is For Official Use Only. It is available to authorized recipients at https://ca.dtic.mil/cjcs_directives/index.htm

⁷ Available through DoD Lock Program at <https://locks.navfac.navy.mil> at the Documents, Federal Specifications tab for Federal Specifications or Documents, Directives and Guidance tab for Federal Standards and Military Handbooks.

⁸ Available through GSA at [http://www.gsa.gov/portal/content/103856#Federal Specifications](http://www.gsa.gov/portal/content/103856#Federal%20Specifications)

- (as) National Security Agency/Central Security Service Evaluated Product List 02-01, “NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders” (also Annex A to NSA/CSS Specification 02-01, “High Security Crosscut Paper Shredders”), current edition
- (at) National Security Agency/Central Security Service Evaluated Product List 02-02, “NSA/CSS Evaluated Products List for High Security Disintegrators” (also Annex A to NSA/CSS Specification 02-02, “High Security Disintegrators”), current edition
- (au) Military Handbook 1013/1A, “Design Guidelines for Physical Security of Facilities,” December 15, 1993⁷
- (av) Underwriters Laboratories Inc., Standard 634, “Standard for Connectors and Switches for Use with Burglar-Alarm Systems,” October 12, 2007⁹
- (aw) National Security Agency/Central Security Service Policy Manual 3-16, “Control of Communications Security (COMSEC) Material,” August 2005¹⁰
- (ax) Executive Order 13549, “Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities,” August 18, 2010
- (ay) Committee on National Security Systems, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 7003, “Protective Distribution Systems (PDS),” December 13, 1996
- (az) DoD Instruction 5200.33, “Defense Courier Operations,” June 30, 2011
- (ba) DoD 5220.22-R, “Industrial Security Regulation,” December 4, 1985
- (bb) Chapter I of title 39, Code of Federal Regulations
- (bc) DoD Instruction 8523.01, Communications Security (COMSEC), April 22, 2008
- (bd) Intelligence Community Directive 503, “Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,” September 15, 2008¹¹
- (be) Department of Defense Foreign Clearance Manual, September 5, 2011¹²
- (bf) DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
- (bg) DoD 5105.38-M, “Security Assistance Management Manual (SAMM),” October 3, 2003
- (bh) DoD Directive 8570.01, “Information Assurance Training, Certification, and Workforce Management,” August 15, 2004
- (bi) DoD Instruction 3305.13, “DoD Security Training,” December 18, 2007
- (bj) DoD Instruction O-5205.11, “Management, Administration, Oversight of DoD Special Access Programs (SAPs),” July 1, 1997
- (bk) Section 2723 of title 10, United States Code
- (bl) Intelligence Community Directive 701, “Security Policy Directive for Unauthorized Disclosures of Classified Information,” March 14, 2007¹³
- (bm) Sections 102, 105, 552¹⁴ and 552a¹⁵ of title 5, United States Code
- (bn) DoD Directive 5230.24, “Distribution Statements on Technical Documents,” March 18, 1987

⁹ Available from Underwriters laboratories Inc. at <http://www.ul.com/global/eng/pages/solutions/standards>

¹⁰ Available to authorized recipients at www.iad.nsa.smil.mil/resources/library/nsa_office_of_policy_section/index.cfm

¹¹ Available at http://www.dni.gov/electronic_reading_room/ICD_503.pdf

¹² Available at <https://www.fcg.pentagon.mil>

¹³ Available on JWICS at <http://www.intelink.ic.gov/sites/ppr/policyHome/default.aspx>

¹⁴ Also known and referred to in this volume as “The Freedom of Information Act (FOIA),” as amended

¹⁵ Also known and referred to in this volume as “The Privacy Act of 1974, as amended”

- (bo) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011
- (bp) Committee on National Security Systems, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4003, "Reporting and Evaluating COMSEC Incidents," December 2, 1991¹⁶
- (bq) Section 3161 of Public Law 105-261, "National Defense Authorization Act for Fiscal Year 1999," as amended
- (br) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007
- (bs) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
- (bt) Committee on National Security Systems Policy 18, "National Policy on Classified Information Spillage," June 2006¹⁶
- (bu) Committee on National Security Systems Instruction 1001, "National Instruction on Classified Information Spillage," February 2008¹⁶
- (bv) Assistant Secretary of Defense for Command, Control, Communications and Intelligence Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001
- (bw) Assistant Secretary of Defense for Networks and Information Integration Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," July 3, 2007
- (bx) Assistant Secretary of Defense for Networks and Information Integration Memorandum, "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
- (by) Director, Administration and Management Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifying Information," September 25, 2008
- (bz) Directive-Type Memorandum 09-026, "Responsible and Effective Use of Internet-based Capabilities," February 25, 2010
- (ca) DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004
- (cb) DoD Instruction 5210.02, "Access to and Dissemination of Restricted Data and Formerly Restricted Data," June 3, 2011
- (cc) Deputy Secretary of Defense Memorandum, "Protection of NATO Classified Information Stored, Processed or Transmitted in U.S. Communication and Information (CIS) Systems and Networks," September 8, 2000
- (cd) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 7, 1998
- (ce) DoD Instruction 5200.39, "Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008
- (cf) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
- (cg) Section 403 of title 50, United States Code (also known as "The National Security Act of 1947," as amended)
- (ch) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
- (ci) DoD 5220.22-C, "Carrier Supplement to Industrial Security Manual for Safeguarding Classified Information," October 1, 1986

¹⁶ NTISSI and documents issued by the Committee on National Security Systems (CNSS) are available at www.cnss.gov/full-index.html

- (cj) Section 2162 of title 42, United States Code (also known as “The Atomic Energy Act of 1954,” as amended)
- (ck) DoD Instruction 5025.01, “DoD Directives Program,” September 26, 2012

ENCLOSURE 2

SAFEGUARDING

1. CONTROL MEASURES. DoD Components shall have a system of control measures that ensure access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which access occurs and to the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures, which may include records of internal distribution, access, generation, inventory, reproduction, and disposition, shall be required when technical, physical, and personnel control measures are insufficient to deter and detect access by unauthorized persons. Except as otherwise specified, requests for waivers to the provisions of this Volume shall be submitted in accordance with section 16 of Enclosure 3 of Volume 1.

2. PERSONAL RESPONSIBILITY FOR SAFEGUARDING. Everyone who works with classified information is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to classified information. Everyone granted access to classified information is personally responsible for protecting the classified information they know, possess, or control and for complying with the pre-publication security review processes specified in DoDD 5230.09 (Reference (k)). Classified information shall be protected at all times either by storing it as this Volume prescribes or by having it under the personal observation and control of an authorized individual.

3. ACCESS TO CLASSIFIED INFORMATION. Except as provided in sections 5 and 6 of this enclosure and in accordance with section 11 of Enclosure 3 of Volume 1, no person may have access to classified information unless that person has a security clearance in accordance with DoD 5200.2-R (Reference (l)) and has signed a Standard Form (SF) 312, "Classified Information Non-Disclosure Agreement" (NDA), and access is essential to the accomplishment of a lawful and authorized Government function (i.e., has a need to know).

4. DETERMINING NEED FOR ACCESS. The individual with authorized possession, knowledge, or control of the information has the final responsibility for determining whether a prospective recipient's official duties requires them to possess or have access to any element or item of classified information, and whether that prospective recipient has been granted the appropriate security clearance by proper authority.

5. EMERGENCY AUTHORITY. In emergencies in which there is an imminent threat to life or in defense of the homeland, the Heads of the DoD Components may authorize the disclosure of classified information, including information normally requiring the originator's prior authorization, to an individual or individuals who are otherwise not routinely eligible for access. The disclosing authority shall:

- a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose.
- b. Limit the number of individuals who receive classified information.
- c. Transmit the classified information through approved Federal government channels by the most secure and expeditious method consistent with this Volume, or by other means deemed necessary when time is of the essence.
- d. Provide instructions about what specific information is classified and how it should be safeguarded. Information disclosed shall not be deemed declassified as of result of such disclosure or subsequent use by a recipient. Physical custody of classified information must remain with an authorized Federal government entity in all but the most extraordinary circumstances.
- e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information to unauthorized individuals and obtain a signed SF 312.
- f. Notify the agency or DoD Component originating of the information and the Deputy Under Secretary of Defense for Intelligence, and Security (DUSD(I&S)) within 72 hours of the disclosure of classified information, or at the earliest opportunity that the emergency permits but no later than 30 days after the release, by providing:
 - (1) A description of the disclosed information.
 - (2) Identification of individuals to whom the information was disclosed.
 - (3) How the information was disclosed and transmitted.
 - (4) Reason for the emergency release.
 - (5) How the information is being safeguarded.
 - (6) A description of the briefings provided.
 - (7) A copy of the signed SF(s) 312.

6. ACCESS BY INDIVIDUALS OUTSIDE THE EXECUTIVE BRANCH. Classified information may be made available to individuals or agencies outside the Executive Branch, as provided in this section, if such information is necessary for performance of a lawful and authorized function, and such release is not prohibited by the originating department or agency. The Heads of DoD Components shall designate officials to ensure the recipient's eligibility for access, prior to the release of classified information. (See Volume 1, Enclosure 3, section 11 for requirements for access by individuals inside the Executive Branch.)

a. Congress. DoDI 5400.04 (Reference (m)) provides rules for access to classified information or material by Congress, its committees, members, and staff representatives. Members of Congress, by virtue of their elected position, are not investigated or cleared by the Department of Defense.

b. Government Printing Office (GPO). Collateral documents and material of all classifications may be processed by the GPO, which protects the information according to a DoD/GPO Security Agreement (Reference (n)).

c. Representatives of the Government Accountability Office (GAO). DoDI 7650.01 (Reference (o)) sets forth rules for granting GAO representatives access to classified information that the Department of Defense originates and possesses when such information is relevant to the performance of the statutory responsibilities of that organization. Certifications of security clearances and the basis therefore, shall be accomplished under arrangements between the GAO and the relevant DoD Component. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes, but not for access to classified information.

d. Historical Researchers. Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that the DoD Component Head or senior agency official with classification jurisdiction over the information:

(1) Determines, in writing, that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted by certifying that the requester has been found to be eligible for access pursuant to Reference (1) and section 3 of this enclosure.

(2) Limits access to specific categories of information over which the DoD Component has classification jurisdiction or for which the researcher has the written consent of the DoD Component or non-DoD agency with classification jurisdiction. The information contained within or revealed by the specified categories must be within the scope of the research.

(3) Maintains custody of the classified material at a DoD installation or activity or authorizes access to documents held by the National Archives and Records Administration (NARA).

(4) Obtains the requester's agreement to safeguard the information and to submit any notes and manuscripts intended for public release for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction to determine whether classified information is contained therein. The agreement shall be documented by execution of a statement substantially similar to that in Figure 1.

Figure 1. Conditions Governing Access to Official Records by Historical Researchers

To Whom It May Concern:

I understand that the classified information to which I have requested access for historical research purposes is concerned with the national defense or foreign relations of the United States. Unauthorized disclosure could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to the national security depending on whether the information is classified Confidential, Secret, or Top Secret, respectively. If granted access, I therefore agree to the following conditions governing access to the [insert Component or activity] files:

1. I will abide by any rules and restrictions issued in your letter of authorization, including those of other Agencies whose information is interfiled with that of the [insert Component or activity].
2. I agree to safeguard the classified information to which I gain possession or knowledge in a manner consistent with Part 4 of Executive Order 13526, "Classified National Security Information," and the applicable provisions of the DoD regulations concerning safeguarding classified information, including Volumes 1, 2, and 3 of DoD Manual 5200.01, "DoD Information Security Program."
3. I agree not to reveal to any person or Agency any classified information obtained because of this access except as authorized in the terms of your authorization letter or a follow-on letter. I further agree that I shall not use the information for purposes other than those set forth in my request for access.
4. I agree to submit my research notes for review to determine if classified information is contained in them before their removal from the specific area assigned to me for research. I further agree to submit my manuscript(s) for a security review before its publication or presentation. In each of these reviews, I agree to comply with any decision of the reviewing official in the interests of the security of the United States, including the retention or deletion of any classified parts of such notes and manuscript whenever the Federal Agency concerned deems such retention or deletion necessary.
5. I understand that failure to abide by the conditions in this statement shall constitute sufficient cause for canceling my access to classified information and for denying me any future access and may subject me to criminal provisions of Federal Law as referred to in Item 6.
6. I have been informed that provisions of title 18 of the United States Code impose criminal penalties, under certain circumstances, for the unauthorized disclosure, loss, copying, or destruction of defense information.

THIS STATEMENT IS MADE TO THE UNITED STATES GOVERNMENT TO ENABLE IT TO EXERCISE ITS RESPONSIBILITY FOR THE PROTECTION OF INFORMATION AFFECTING THE NATIONAL SECURITY. I UNDERSTAND THAT ANY MATERIAL FALSE STATEMENT THAT I MAKE KNOWINGLY AND WILLFULLY SHALL SUBJECT ME TO THE PENALTIES OF TITLE 18, U.S. CODE, SECTION 1001.

Signature:

Witness's Signature:

Date:

(5) Authorizes access, in writing, for no more than 2 years from the date of issuance. The DoD Component may renew access for 2-year periods in accordance with DoD Component-issued regulations.

e. Presidential or Vice Presidential Appointees and Designees. Persons who previously occupied senior policy-making positions to which they were appointed or designated by the President or Vice President may not remove classified information upon departure from office, as all such material shall remain under the U.S. Government's security control. Such persons may be authorized access to classified information they originated, reviewed, signed, received, or that was addressed to them while serving as an appointee or designee, provided that the DoD Component Head or senior agency official with classification jurisdiction for such information:

(1) Determines, in writing, that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted and by certifying that the requester has been found to be eligible for access pursuant to section 3 of this enclosure.

(2) Limits access to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

(3) Retains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the NARA.

(4) Obtains the requestor's agreement (SF 312) to safeguard the information and to submit any notes and manuscript for pre-publication review by all DoD Components and non-DoD departments or agencies with classification jurisdiction to determine that no classified information is contained therein.

f. Use of Classified Information in Litigation. DoDD 5405.2 (Reference (p)) governs the use of classified information in litigation.

g. Special Cases. When necessary in the interests of national security, the Heads of the DoD Components or their senior agency official may authorize access to classified information by persons outside the Federal government, other than those enumerated in section 5 of this enclosure and paragraphs 6.a through 6.f of this section. Prior to authorizing access, such official must determine that the recipient is reliable, loyal, and trustworthy for the purpose of accomplishing a national security objective; meets the requirements of section 3 of this enclosure; and can and will safeguard the information from unauthorized disclosure. The national security objective shall be stated in the authorization, which shall be in writing. This authority may not be further delegated.

7. VISITS. The Heads of the DoD Components shall establish procedures to accommodate visits to their Component facilities involving access to, or disclosure of, classified information. As a minimum, these procedures shall include verifying the identity, personnel security clearance, access (if appropriate), and need to know for all visitors.

a. Visit requests shall be processed and security clearance and access level verified using the Joint Personnel Adjudication System (JPAS) for DoD civilian, military, and contractor personnel whose access level and affiliation are reflected in JPAS. Fax, telephone, or other appropriate method shall be used for those personnel whose access level and affiliation are not reflected in JPAS.

b. Visits by foreign nationals to DoD Components and facilities, except for activities or events that are open to the public, shall be handled in accordance with DoDD 5230.20 (Reference (q)) and documented in the Foreign Visits System Confirmation Module.

8. PROTECTION WHEN REMOVED FROM STORAGE. An authorized person shall keep classified material removed from storage under constant surveillance. Classified document cover sheets (SF 703, "Top Secret (Cover sheet);" SF 704, "Secret (Cover sheet);" or SF 705 "Confidential (Cover sheet)") shall be placed on classified documents not in secure storage. The cover sheets show, by color and other immediately recognizable format or legend, the applicable classification level.

9. END OF DAY SECURITY CHECKS. The heads of activities that process or store classified information shall establish a system of security checks at the close of each duty and/or business day to ensure that any area where classified information is used or stored is secure. SF 701, "Activity Security Checklist," shall be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms, and containers used for storing classified material. SF 702, "Security Container Check Sheet," shall be used to record such actions. SFs 701 and 702 shall be retained and disposed of as required by Component records management schedules.

10. EMERGENCY PLANS. Plans shall be developed to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of compromise, and for the recovery of classified information, if necessary, following such events. The level of detail and the amount of testing and rehearsal of these plans shall be determined by assessing the risk of hostile action, foreign intelligence threats, natural disaster, or terrorist activity that may place the information in jeopardy.

a. Use the requirements of Committee on National Security Systems (CNSS) Instruction 4004 (Reference (r)) when developing plans for the emergency protection (including emergency destruction under no-notice conditions) of classified communications security (COMSEC) material.

b. When preparing emergency plans, consider:

(1) Reducing the amount of classified material on hand.

(2) Storing less frequently used classified material at other secure locations.

(3) Creating regular back up copies of information in electronic formats for off-site storage.

(4) Transferring as much retained classified information to removable electronic media as possible, thereby reducing its bulk.

11. USE OF SECURE COMMUNICATIONS. In accordance with the requirements of Enclosure 4, classified information shall be transmitted only over secure communications circuits approved for transmission of information at the specified level of classification. This includes communication by telephone, facsimile, e-mail and other forms of electronic communications (e.g., messages, websites). See Volume 2 of this Manual for guidance on required markings.

12. REMOVAL OF CLASSIFIED INFORMATION FOR WORK AT HOME. When it is mission critical for individuals to remove classified information and materials (e.g., IT equipment and associated storage media) for work at home, specific security measures and approvals are required. Security measures appropriate for the level of classification must be in place to provide adequate protection and security-in-depth and to prevent access by unauthorized persons. Compliance with section 13 of Enclosure 4 of this Volume is also required.

a. Top Secret. Only the Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commanders, or the senior agency officials appointed pursuant to section 5.4(d) of Reference (d) may authorize the removal of Top Secret information from designated working areas for work at home. Such officials may also authorize removal of information for work at home for any lower level of classification.

b. Secret and Confidential. The Heads of the DoD Components may authorize removal of Secret and Confidential information from designated working areas for work at home. This authority shall not be delegated below the major command or equivalent level.

c. Residential Storage Equipment. A General Services Administration (GSA)-approved security container shall be furnished for residential storage of classified information. Written procedures shall be developed to provide for appropriate protection of the information, including a record of the classified information that has been authorized for removal for work at home.

d. Classified IT Systems. See section 7 of Enclosure 7 of this Volume when classified IT equipment will be used. All residential classified network connections must be certified and accredited in accordance with DoDI 8510.01 (Reference (s)) requirements.

e. Foreign Country Restriction. Work at home may be authorized in foreign countries only when the residence is in a specific location where the United States enjoys extraterritorial status (e.g., on the embassy, chancery, or consulate compound) or on a U.S. military installation.

13. WORKING PAPERS. Working papers are documents (e.g., notes, drafts, prototypes) or materials (e.g., printer ribbons, photographic plates), regardless of the media, created during development and preparation of a finished product. Working papers and materials are not intended or expected to be disseminated. Working papers and materials containing classified information shall be:

- a. Dated when created.
- b. Marked with the highest classification of any information contained therein.
- c. Safeguarded as required for the assigned classification.
- d. Conspicuously marked “Working Paper” on the cover and/or first page of the document or material (or comparable location for special types of media) in letters larger than existing text.
- e. Destroyed in accordance with chapter 33 of title 44, U.S.C. (Reference (t)) as implemented by DoDD 5015.2 (Reference (u)) and appropriate DoD Component implementing directives and records schedules when no longer needed.
- f. Marked and controlled the same way as this Manual requires for finished products of the same classification when retained more than 180 days from date of origin (30 days for SAPs), filed permanently, e-mailed within or outside the originating activity, or released outside the originating activity, except as provided in paragraph 13.g. of this section.
- g. Shared between action officers, either physically or electronically, without controlling them as permanent documents only when:
 - (1) The working materials are shared informally (e.g., collaborative documents or coordinating drafts) in the development process.
 - (2) Transfer or transmission of the material is via secure means and, if electronic, by means other than e-mail.
 - (3) All copies held by other than the originator are marked and controlled as required for finished products when retained more than 180 days of origin (30 days for SAPs). Consult with the originator for correct markings.

14. EQUIPMENT USED FOR PROCESSING CLASSIFIED INFORMATION. The Department of Defense has a variety of non-COMSEC-approved equipment that is used to process classified information. This includes copiers, facsimile machines, computers and other IT equipment and peripherals, display systems, and electronic typewriters. Activities shall identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Activity security procedures shall prescribe the appropriate safeguards to:

a. Prevent unauthorized access to that information, including by repair or maintenance personnel.

b. Ensure that repair procedures do not result in unauthorized dissemination of or access to classified information. Where equipment cannot be properly sanitized or appropriately knowledgeable escort provided, cleared maintenance technicians shall be used. Electronic repair or diagnostic equipment shall be maintained as classified material by the DoD Component if there is the potential for classified data transmission from the equipment being serviced. Use of remote diagnostic or repair capabilities shall be specifically approved and authorized in writing by the activity security manager; if the equipment retains or stores any classified information appropriate physical and logical protection must be provided on the remote end and secure communications are required.

c. Replace and destroy equipment parts in the appropriate manner when classified information cannot be removed. Removable disk drives, memory chips and boards, and other electronic components of copiers, fax machines, etc. may be sanitized or destroyed in the same manner as used for comparable computer equipment. Alternatively, the equipment shall be designated as classified and be retained and protected accordingly.

d. Ensure that appropriately knowledgeable, cleared personnel inspect equipment and associated media used to process classified information before the equipment is removed from protected areas to ensure there is no retained classified information. Classification markings and labels shall be removed from sanitized equipment and media after inspection, prior to removal from protected areas.

e. Ensure computers and other equipment used to process classified information or to transmit classified information across a network are certified and accredited in accordance with Reference (s) as required by DoDD 8500.01E (Reference (v)). Measures to protect against compromising emanations shall be implemented in accordance with DoDD C-5200.19 (Reference (w)).

15. REPRODUCTION OF CLASSIFIED MATERIAL. Paper copies, electronic files, and other material containing classified information shall be reproduced only when necessary for accomplishing the organization's mission or for complying with applicable statutes or Directives. Use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

a. Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced, including by e-mailing, scanning, and copying, to the extent operational needs require.

b. The DoD Components shall establish procedures that facilitate oversight and control of the reproduction of classified information and the use of equipment for such reproduction, including controls that ensure:

- (1) Reproduction is kept to a minimum consistent with mission requirements.
- (2) Personnel reproducing classified information are knowledgeable of the procedures for classified reproduction and aware of the risks involved with the specific reproduction equipment being used and the appropriate countermeasures they are required to take.
- (3) Reproduction limitations originators place on documents and special controls applicable to special categories of information are fully and carefully observed.
- (4) Reproduced material is placed under the same accountability and control requirements as applied to the original material. Extracts of documents will be marked according to content and may be treated as working papers if appropriate.
- (5) Reproduced material is conspicuously identified as classified at the applicable level and copies of classified material are reviewed after the reproduction process to ensure that the required markings exist.
- (6) Waste products generated during reproduction are protected and destroyed as required.
- (7) Classified material is reproduced only on approved and, when applicable, properly accredited systems. Section 14 of this enclosure provides additional guidance.
- (8) Foreign government information (FGI) is reproduced and controlled pursuant to guidance and authority granted by the originating government.

16. CLASSIFIED MEETINGS AND CONFERENCES. Meetings and conferences involving classified information present special vulnerabilities to unauthorized disclosure. The Heads of the DoD Components shall establish specific requirements for protecting classified information at DoD Component-sponsored meetings and conferences, to include seminars, exhibits, symposia, conventions, training classes, workshops, or other such gatherings, during which classified information is disseminated.

- a. DoD Component approval processes shall ensure that the following requirements are met:
 - (1) The meeting or conference serves a specified U.S. Government purpose.
 - (2) Use of other approved methods or channels for disseminating classified information or material are insufficient or impractical.
 - (3) The meeting or conference, or classified sessions thereof, takes place only at an appropriately cleared U.S. Government facility or a U.S. contractor facility that has an appropriate facility security clearance and, as required, secure storage capability, unless an exception is approved, in writing, in advance by the DoD Component Head or senior agency

official. Such exception authority shall not be delegated below the senior agency official. Requests for exceptions to permit use of facilities other than appropriately cleared U.S. Government or U.S. contractor facilities shall be submitted to the DoD Component Head or senior agency official in accordance with Component procedures. The request shall include a security plan that describes how the requirements of paragraphs 16.b and 16.d of this section shall be met.

(a) If classified meetings or conferences occur at a cleared U.S. contractor location, the contractor shall comply with all applicable portions of DoD 5220.22-M (Reference (x)) and parts 120 through 130 of title 22, CFR (Reference (y)) (also known as “The International Traffic in Arms Regulations”). DoD approval for the conduct of the meeting does not constitute authorization for presentation of export-controlled information when foreign nationals attend.

(b) The conduct of classified meetings or conferences at foreign installations and contractor sites is often subject to the rules and regulations of the host country, thus presenting additional security risks. Prior to approval of the conduct of such meetings, the DoD Component shall obtain assurances, in writing, that the responsible foreign government will agree to use security measures and controls that are at least as stringent as those required by this Manual. The provisions of paragraph 16.d. also shall be satisfied. To this end, assistance can be provided by the Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy (OUSDP).

(c) Routine day-to-day meetings and gatherings of DoD officials shall be conducted only at an appropriately cleared U.S. Government or contractor facility. Exceptions shall not be granted for routine meetings.

(d) The provisions of this section do not apply to operational meetings conducted in combat situations, classes conducted by DoD schools, or gatherings of personnel of a DoD Component and foreign government representatives or U.S. and/or foreign contractor representatives on a matter related to a specific U.S. Government contract, program, or project.

(4) Classified sessions are segregated from unclassified sessions.

(5) Access to the meeting or conference, or specific sessions thereof, where classified information may be discussed or disseminated is limited to persons who possess an appropriate security clearance and need to know.

(6) Any participation by foreign nationals or foreign representatives complies with requirements of Reference (q) and DoDD 5230.11 (Reference (z)) (e.g., the responsible U.S. Government foreign disclosure office(s) assures, in writing, that the information to be presented has been approved for disclosure to the represented foreign countries).

(7) Announcement of the meeting or conference is unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

(8) Procedures shall ensure that classified information, documents, recordings, audiovisual material, information systems, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as provisions of this Manual require. Recording or taking notes, including notes on classified electronic devices, during classified sessions shall be permitted only when it is determined that such action is necessary to fulfill the U.S. Government purpose for the meeting.

(9) Information systems used during the meeting or conference to support creation or presentation of classified information shall meet all applicable requirements for processing classified information, including as appropriate considerations of technical security countermeasures (TSCM). Unclassified laptop computers, handheld information technologies (e.g., personal electronic devices (PEDs)), and other similar devices shall not be used for note taking during classified sessions. Use of classified computers and other electronic devices shall be permitted only when needed to meet the intent of the meeting or conference and appropriate protection and TSCM requirements have been met.

b. The DoD activity sponsoring a classified meeting or conference shall assign an official to serve as security manager for the meeting and be responsible for ensuring that, at a minimum, the following security provisions are met:

(1) Attendees are briefed on safeguarding procedures.

(2) Entry is controlled so that only authorized personnel gain entry to the area. Particular caution shall be taken to ensure that any individual who is not authorized to attend the classified session(s) is denied entry thereto.

(3) The perimeter is controlled to ensure unauthorized personnel cannot overhear classified discussions or introduce devices that would result in the compromise of classified information.

(4) Escorts are provided for uncleared personnel who are providing services to the meeting or conference (e.g., setting up food or cleaning) when classified presentations and/or discussions are not in session.

(5) Use of cell phones, PEDs, 2-way pagers, and other electronic devices that transmit is prohibited.

(6) Classified notes and handouts are safeguarded in accordance with Enclosure 3.

(7) Classified information is disclosed to foreign nationals only in accordance with the provisions of Reference (z).

(8) An inspection of the room(s) is conducted at the conclusion of the meeting or conference (or at the end of each day of a multi-day event) to ensure all classified materials are properly stored.

c. Appropriately cleared U.S. Government contractor personnel may provide administrative support and assist in organizing a classified meeting or conference, but the DoD Component sponsoring the gathering remains responsible for all security requirements.

d. Facilities other than appropriately cleared U.S. Government or U.S. contractor facilities proposed for use for classified meetings and conferences shall:

(1) Not be open to the public and access shall be controlled by the U.S. Government or cleared contractor through a 100 percent identification card check at the perimeter point. For a military installation or comparably protected Federal government compound, this can be at the perimeter fence of the installation or compound.

(2) Have the room(s) where the classified sessions are to be held located away from public areas so that access to the room(s), walls, and ceiling(s) can be completely controlled during the classified sessions.

(3) Provide authorized means to secure classified information in accordance with Enclosure 3.

(4) Meet the DoD antiterrorism standards specified by DoDI 2000.16 (Reference (aa)).

(5) Be subject to TSCM surveys in accordance with DoDI 5240.05 (Reference (ab)). When addressing this requirement, TSCM security classification guidance **MUST** be consulted to ensure proper classification of meeting details when associated with the use of TSCM.

e. Not later than 90 days following the conclusion of a classified meeting or conference for which an exception was granted, the sponsoring activity shall provide an after-action report to the DUSD(I&S) through the approving DoD Component Head or senior agency official. The after-action report shall be a brief summary of any issues or threats encountered during the event and actions taken to address the situation.

17. SAFEGUARDING FGI

a. North Atlantic Treaty Organization (NATO) Information. NATO classified information shall be controlled and safeguarded according to United States Security Authority for NATO Instruction 1-07 (Reference (ac)).

b. Other FGI. See the Glossary for the definition of FGI.

(1) To avoid inadvertent compromise, classified FGI shall be stored in a manner that will avoid commingling with other material. For small volumes of material, separate files in the same vault, container, or drawer will suffice.

(2) FGI shall be re-marked if needed to ensure the protective requirements are clear. FGI may retain its original classification if it is in English. However, when the foreign

government marking is not in English, or when the foreign government marking requires a different degree of protection than the same U.S. classification designation, a U.S. marking that results in a degree of protection equivalent to that required by the foreign government shall be applied. See Appendix 1 to Enclosure 4 of Volume 2 of this Manual for comparable U.S. classification designations.

(3) U.S. documents containing FGI shall be marked as required by section 9 of Enclosure 4 of Volume 2 of this Manual. The foreign government document or authority on which derivative classification is based must be identified on the "Derived from:" line, in addition to the identification of any U.S. classification authority. A continuation sheet should be used for multiple sources, if necessary. A U.S. document containing FGI cannot be declassified or downgraded below the highest level of FGI contained in the document without the written permission of the foreign government or international organization that originated the information.

(4) Security clearances issued by the U.S. Government are valid for access to classified FGI of a comparable level.

(5) The transmission of FGI within the United States among U.S. Government agencies and U.S. contractors and between U.S. contractors with a need to know must be in accordance with this Manual and Reference (x).

(6) The international transfer of foreign government classified information must be by government officials through government-to-government channels, or channels agreed upon in writing by the originating and receiving governments (collectively "government-to-government transfer"). See Enclosure 4 and its Appendix for further guidance on transfer of classified information.

(7) The receiving DoD Components shall protect FGI to at least a degree equivalent to that required by the foreign government or international organization that provided the information. FGI shall be controlled and safeguarded in the same manner as prescribed for U.S. classified information, except as described below. The control and safeguarding requirements for FGI may be modified as permitted by a treaty or international agreement, or, for foreign governments with which there is no treaty or international agreement, through formal written agreement between the responsible national security authorities or designated security authorities of the originating and receiving governments (hereafter referred to collectively as designated security authorities (DSAs)). The Under Secretary of Defense for Policy (USD(P)) serves as the DSA.

(a) Control of Foreign Government Top Secret Information. Maintain records for 5 years of the receipt, internal distribution, destruction, annual inventory, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction shall be witnessed.

(b) Control of Foreign Government Secret Information. Maintain records for 3 years of the receipt, distribution, external dispatch, reproduction, and destruction of material

containing foreign government Secret information. Other records may be necessary if the originator requires. Secret FGI may be reproduced to meet mission requirements.

(c) Control of Foreign Government Confidential Information. Maintain records for 2 years for the receipt and external dispatch of Confidential FGI. Do not maintain other records for foreign government Confidential information unless required by the originating government. Confidential FGI may be reproduced to meet mission requirements.

(d) Foreign Government Restricted Information and Information Provided in Confidence. In order to ensure the protection of Restricted FGI or foreign government unclassified information provided in confidence, such information shall be classified in accordance with Reference (d) which states that unauthorized disclosure of FGI is presumed to cause damage to the national security. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the information shall be marked "CONFIDENTIAL-Modified Handling" as described in Volume 2, Enclosure 4, paragraph 4.c of this Manual and the following requirements shall also be met:

1. The information shall be provided only to those individuals who have an established need to know, and where access is required by official duties.

2. Individuals given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet.

3. Documents shall be stored to prevent unauthorized access (e.g., a locked desk or cabinet or a locked room to which access is controlled).

4. DoD Components and contractors performing on DoD contracts shall handle documents bearing the marking "UK RESTRICTED" as classified in accordance with subparagraph 17.b.(7)(d). The provision in the U.S./United Kingdom (UK) Security Implementing Arrangement (Reference (ad)) that allows documents marked "UK RESTRICTED" to be handled in a manner similar to For Official Use Only (FOUO) information applies ONLY to DoD contractors operating under COMMERCIAL contracts with the UK and, pursuant to the agreement, the UK must include in the applicable contract its requirements for the marking and handling of the information. The provision does NOT apply to, nor permit, such handling of UK RESTRICTED information by DoD Components or by contractors when performing on DoD contracts.

(8) FGI shall not be disclosed to nationals of third countries, including foreign nationals who are protected individuals or permanent resident aliens, or to any other third party, or used for other than the purpose for which the foreign government provided it without the originating government's written consent. Questions regarding releasability or disclosure should be directed to the U.S. originator, who will consult with the foreign government as required. Contractors will submit their requests through the contracting U.S. Government agency for U.S. contracts and the Defense Security Service for direct commercial contracts. Approval from the originating government does not eliminate the requirement for the contractor to obtain an export

authorization as required by other regulations or policies.

18. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM). A Head of a DoD Component with original classification authority (OCA) may employ ACCM when he or she determines that the standard security measures detailed in this Manual are insufficient to enforce need to know for classified information and SCI or SAP protections are not warranted. The use of an unclassified nickname, obtained in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150.29C (Reference (ae)), together with a list of persons authorized access, and a specific description of information subject to the enhanced ACCM controls, are the three requisite elements of an ACCM.

a. DoD Proponents for ACCM. The DoD staff proponent for ACCM management, oversight and Congressional reporting is the OUSD(P). The proponent for ACCM security policy is the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). Given this sharing of ACCM responsibilities, staff elements in OUSD(P) and OUSD(I) shall implement mechanisms that ensure transparency of all ACCM actions.

b. ACCM Approval. A Head of a DoD Component may approve ACCM use for classified information over which they have cognizance. Prior to approving the establishment of an ACCM, the criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and a countermeasures cost benefits analysis shall be assessed.

c. Guidance on ACCM Use. Use of ACCM must be consistent with the following guidance:

(1) ACCM may be used to assist in enforcing need to know for classified DoD intelligence matters. The DoD Component Head establishing or terminating any such ACCM shall provide written notification within 30 days to the Director of Security, OUSD(I), and the Director, Special Programs, OUSD(P), who shall maintain this information as long as the ACCM is in use.

(2) ACCM may be used to assist in enforcing need to know for classified operations, sensitive support, and other non-intelligence activities. The DoD Component Head establishing or terminating any such ACCM shall provide written notification within 30 days to the Director, Special Programs, OUSD(P), for review. The Director, Special Programs, OUSD(P), shall maintain this information as long as the ACCM is in use.

(3) ACCM shall not be used for acquisition programs or activities progressing through the acquisition process.

(4) DoD Components shall obtain an unclassified nickname consistent with Reference (ae) and coordinate with OUSD(P) to preclude duplication of nicknames.

(5) A roster or listing of all persons accessed to the ACCM shall be maintained by the ACCM control officer (see subparagraph 18.f.(1)(c) of this section). The access roster will differentiate between those persons actively accessed and those whose accesses are currently

inactive.

(6) ACCM documents and materials shall be marked as specified in Enclosure 4 of Volume 2 of this Manual.

(7) Heads of DoD Components must establish and maintain a system that provides for recurrent inspection of the ACCM they have approved. This mechanism shall ensure compliance with the provisions of this Manual. Each ACCM shall be overseen and inspected on a recurrent basis by the ACCM sponsor or OUSD(P).

d. Prohibited Security Measures. The application of the following security measures with ACCM material is prohibited:

(1) Using personnel security investigative or adjudicative standards that are more stringent than those normally required for a comparable level of classified information to establish access eligibility to ACCM-protected information.

(2) Using code words as defined in Reference (ae).

(3) Using trigraphs, digraphs, or other abbreviations of the approved nickname.

(4) Using specialized non-disclosure agreements or any certificates of disclosure or non-disclosure for ACCM access.

(5) Using a billet structure or system to control the position or numbers of persons afforded ACCM access.

e. Prohibited Uses of ACCM. The following uses of ACCM are prohibited:

(1) Using ACCM for NATO or non-intelligence FGI. For NATO, exceptions to this limitation can be granted only by the Secretary of Defense. For non-intelligence FGI, exceptions to this limitation can be granted only by the USD(P). Request for exceptions shall be forwarded to the Director, International Security Programs, Defense Technology Security Administration, OUSD(P), for action. Such approvals must be documented and retained by the sponsor.

(2) Using ACCM to protect classified information in acquisition programs as defined in DoDD 5000.01 (Reference (af)).

(3) Using ACCM to protect technical or operational requirements of systems in the acquisition process. Systems in operational use are not viewed as being in the acquisition process. Components of operational systems are fielded end items, not items in the acquisition process, and improvements to fielded items are eligible for ACCM status if properly justified.

(4) Using ACCM to protect Restricted Data (RD), Formerly Restricted Data (FRD), COMSEC, SCI, SAP, or Nuclear Command and Control Extremely Sensitive Information.

(5) Using ACCM to protect unclassified information.

(6) Using ACCM to preclude or impede congressional, OSD, or other appropriate oversight of programs, command functions, or operations.

(7) Using ACCM to justify funding to procure or maintain a separate ACCM communication system.

f. Documentation

(1) Use of ACCM must be approved in writing by the cognizant DoD Component Head. The correspondence establishing the ACCM shall be signed by the DoD Component Head and shall include the following information:

(a) Unclassified nickname assigned in accordance with Reference (ae).

(b) Designation of the ACCM sponsor. As a minimum, the sponsor shall be a general or flag officer, or senior executive equivalent, who has OCA at the level of or higher than the information protected by the ACCM.

(c) Designation of an ACCM control officer who shall be the organization's point of contact for all matters concerning the ACCM. Subsequent changes in designated personnel shall be provided, in writing, to the Special Programs Office, OUSD(P).

(d) Description of the essential information to be protected by the ACCM.

(e) Effective activation date and expected ACCM duration.

(f) Any planned participation by foreign partners.

(2) The ACCM sponsor shall develop and distribute a program security plan, security classification guide, and program participant briefing to all participating organizations prior to the activation of the ACCM. As a minimum, the briefing will address the specific information that is subject to ACCM security measures.

(3) The Special Programs Office, OUSD(P), shall maintain a central repository of records for all DoD ACCM.

g. Annual Reports of ACCM Use. Not later than December 15 of each year, the DoD Components shall provide a report to OUSD(P) on all ACCM usage during the previous year. The exact format for this report shall be provided annually by OUSD(P), however, the general data elements include: ACCM nickname; purpose and/or description of the ACCM program; expected duration; and ACCM sponsor and ACCM control officer(s).

h. Sharing ACCM-Protected Information. ACCM-protected information may be shared with

other DoD Components and/or other Federal government departments and agencies only when the recipient organization agrees to abide by the ACCM security requirements stipulated in this enclosure.

i. Contractor Access to ACCM. DoD contractors may participate in ACCMs, or be directed to participate, only when such access and the associated security plan are identified in the DD Form 254, "Contract Security Classification Specification." Care must be taken to ensure identification of the security plan does not disclose ACCM-protected data.

j. Program Maintenance

(1) ACCM sponsors shall maintain an updated listing of primary and alternate ACCM control officers for each organization to which they have extended their program.

(2) Each organization's ACCM control officer shall maintain an updated ACCM access control list for their organization.

(3) Initial contact between organizations will be between each organization's ACCM control officers. ACCM control officers may authorize action officer to action officer contact once access control lists have been exchanged between organizations.

(4) Personnel requiring access to ACCM-protected information shall receive specialized training upon initial access to the program and annually thereafter. Training, as a minimum, shall address the procedures for access, control, transmission, storage, and marking. Individuals may be required to sign an acknowledgement of training should the security plan so specify.

(5) ACCM documentation (i.e., program security plan and security classification guide) must be updated a minimum of once every 5 years.

(6) ACCM sponsors shall provide the following information, through the DoD Component Head, to OUSD(P) concurrently with the ACCM annual report:

(a) A listing of primary and alternate ACCM control officers for each organization managing an ACCM.

(b) Any updated ACCM documentation or confirmation that program documentation has been reviewed and is current.

k. Safeguarding ACCM Information. The provisions of this Manual regarding the safeguarding of classified information are modified with respect to use of ACCM as follows:

(1) Top Secret, Secret, and Confidential cover sheets (i.e., SFs 703, 704, and 705, respectively) used to cover ACCM material shall be over stamped or marked with "ACCM" and the appropriate nickname. Cover sheets specifically designated by the DoD Components for use with ACCM must be approved by the Director of Security, OUSD(I), prior to use.

(2) ACCM material should be handled and stored based on the security classification of the information contained therein and in a manner that separates it from non-ACCM classified information. Separate GSA approved storage containers are not required so long as everyone with access to container is also approved for access to the ACCM material stored within, but the measures used (e.g., segregated files, separate folders, drawers labeled for ACCM) shall prevent the commingling of ACCM material with other classified documents.

(3) ACCM information shall be transmitted in the same manner as other classified information at the same classification level with the following exceptions:

(a) ACCM information packaged for transmission shall have the inner envelope marked with the appropriate classification, the caveat "ACCM," and the assigned nickname, and shall be addressed to the attention of an individual authorized access to the ACCM information.

(b) The ACCM nickname shall be used in the text of message traffic and on cover sheets accompanying secure facsimile transmissions to assist in alerting the recipient that the transmission involves ACCM-protected information. Senders shall ensure that an authorized recipient is awaiting the transmission when sending via secure facsimile. When using the Defense Message System (DMS), the material must also be marked as "SPECAT" (Special Category) in accordance with the requirements and procedures in CJCSM 5720.01B (Reference (ag)). Due to limits in DMS processing, only one ACCM nickname should be used in a DMS message.

(c) Automated information systems or electronic files containing ACCM protected information shall be configured with appropriate discretionary access controls to ensure that access is restricted to individuals with authorized access.

(d) Secret Internet Protocol Router Network (SIPRNET) or other secure transmission methods authorized for processing information at the required level of classification may be used to transmit ACCM information. Each such transmission must be marked with the caveat "ACCM" and the authorized nickname in accordance with the marking guidance in Volume 2 and transmitted only to those authorized access to the ACCM information.

(e) The method of transmission selected for ACCM information, whether in hardcopy or electronic form, shall be consistent with the security classification assigned. Designation of information as requiring ACCM protection does not, in and of itself, require the transmission of the information by methods usually reserved for a higher level of classified information.

1. Security Incidents. Compromise of ACCM program information can present an immediate and real threat to national security and those personnel involved in mission execution. Anyone finding ACCM material out of proper control shall take actions to safeguard the material and shall immediately notify the local ACCM control officer, if known, or the local security manager.

(1) All reporting, inquiry, investigation, and damage assessment will be conducted per

the guidelines contained in Enclosure 6 of this Volume. Any reports containing ACCM information shall be handled in accordance with the requirements of this Manual as modified by this section.

(2) Section 13 of Enclosure 6 of this Volume states the actions to take if unauthorized personnel are inadvertently afforded access to ACCM information. Inadvertent disclosure forms, commonly used with compartmented information, are not authorized for use with ACCM information.

(3) Because ACCM program information is not SCI or SAP, reasonable risk management procedures should be followed when ACCM program information is incorrectly placed on non-approved electronic processing systems or electronically transmitted to non-authorized personnel and/or systems. Deleting the file or material from all affected systems is normally a sufficient action unless the material in question is classified at a higher level of classification than that for which the system is accredited.

(4) The ACCM sponsor should be notified when the local inquiry and investigation is completed. Resolution will be in accordance with current guidance contained in Enclosure 6 of this Volume and must consider the guidance contained in the ACCM program security plan. Responsibility for the damage assessment remains with the ACCM sponsor. Any additional action will be as directed by the ACCM sponsor and the local security manager.

m. ACCM Termination. ACCM shall be terminated by the establishing DoD Component when ACCM security measures are no longer required. Notification of ACCM termination must be submitted, in writing, as required by paragraphs 18.c.(1) and 18.c.(2) of this enclosure.

n. Transitioning an ACCM to a SAP. If, at any point in time, the DoD Component Head determines that information protected by ACCM requires further protection as a SAP, authorization to establish a DoD SAP must be requested in accordance with DoD Directive 5205.07 (Reference (ah)).

ENCLOSURE 3

STORAGE AND DESTRUCTION

1. GENERAL REQUIREMENTS

a. Classified information shall be secured under conditions adequate to deter and detect access by unauthorized persons. The requirements specified in this Volume represent acceptable security standards. DoDD 5210.56 (Reference (ai)) specifies DoD policy concerning the use of force for the protection of classified information. Do not store weapons or items such as funds, jewels, precious metals, or drugs in the same container used to safeguard classified information. Holdings of classified material should be reduced to the minimum required to accomplish the mission.

b. GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for storing and protecting classified information. DoDI 3224.03 (Reference (aj)) describes requirements for acquiring physical security equipment for use within the Department of Defense.

c. The DNI establishes security requirements for sensitive compartmented information facilities (SCIFs). These are issued by Reference (i) within the Department of Defense.

d. The DoD Lock Program is designated as the DoD technical authority for locking and storage systems used for the protection of classified information. For technical support, call the DoD Lock Program Technical Support Hotline at 1-800-290-7607 or DSN 551-1212 or review the website at <https://locks.navfac.navy.mil>, for more information.

e. Volume 4 of this Manual specifies storage and destruction requirements for controlled unclassified information.

2. LOCK SPECIFICATIONS. Except as provided elsewhere in this Volume, combination locks on vault doors, secure rooms, and security containers protecting classified information shall conform to Federal Specification FF-L-2740 (hereafter referred to as "FF-L-2740")(Reference (ak)).

3. STORAGE OF CLASSIFIED INFORMATION BY LEVEL OF CLASSIFICATION. Store classified information not under the personal control and observation of an authorized person, in a locked security container, vault, room, or area, as specified in this section.

a. Top Secret. Top Secret information shall be stored:

(1) In a GSA-approved security container with one of the following supplementary

controls:

(a) An employee cleared to at least the Secret level shall inspect the security container once every 2 hours.

(b) The location that houses the security container is protected by an intrusion detection system (IDS) meeting the requirements of the Appendix to this enclosure with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(2) In a GSA-approved security container equipped with a lock meeting FF-L-2740, provided the container is located within an area that has been determined to have security-in-depth (see Glossary for definition);

(3) In an open storage area (also called a secure room) constructed according to the Appendix to this enclosure and equipped with an IDS with the personnel responding to an alarm within 15 minutes of the alarm annunciation if the area has been determined to have security-in-depth, or within 5 minutes of alarm annunciation if it has not;

(4) In a vault, or GSA-approved modular vault, meeting the requirements of Federal Standard (FED-STD) 832 (Reference (al)) as specified in the Appendix to this enclosure; or

(5) Under field conditions during military operations, using such storage devices or security control measures as a military commander deems adequate to prevent unauthorized access. Military commanders should employ risk management methodologies when determining appropriate safeguards.

b. Secret. Secret information shall be stored by one of the following methods:

(1) In the same manner as prescribed for Top Secret information;

(2) In a GSA-approved security container or vault built to FED-STD 832 specifications, without supplementary controls;

(3) In an open storage area meeting the requirements of the Appendix to this enclosure, provided the senior agency official determines in writing that security-in-depth exists, and one of the following supplemental controls is utilized:

(a) An employee cleared to at least the Secret level shall inspect the open storage area once every 4 hours.

(b) An IDS meeting the requirements of the Appendix to this enclosure with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

(4) In a secure room that was approved for the storage of Secret information by the DoD Component prior to October 1, 1995, provided the DoD Component reassesses the requirement for the secure room and makes plans to bring the room up to the standards of subparagraphs

3.b.(1) through 3.b.(3) of this section by October 1, 2013 and provided the area has been determined to have security-in-depth.

c. Confidential. Confidential information shall be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

4. RISK ASSESSMENT. When considering the storage alternatives specified in section 3, a risk assessment shall be performed to facilitate a security-in-depth determination and to aid identification and selection of supplemental controls that may need to be implemented. The analysis should, at a minimum, consider local threats, both known and anticipated, and vulnerabilities; the existing security environment and controls; the ease of access to containers or other areas where classified data is stored; the criticality, sensitivity, and value of the information stored; and cost versus benefits of potential countermeasures. The risk assessment shall be used to determine whether installation of an IDS is warranted or whether other supplemental controls are sufficient.

5. U.S. CLASSIFIED INFORMATION LOCATED IN FOREIGN COUNTRIES. Except for classified information that has been authorized for release to a foreign government or international organization in accordance with Reference (z), and is under that government's or organization's security control, U.S. classified material may be retained and stored in a foreign country only when necessary to satisfy specific U.S. Government requirements. The Heads of the DoD Components shall prescribe requirements for protecting this information, paying particular attention to ensuring proper enforcement of controls on release of U.S. classified information to foreign entities. Compliance with the provisions of this enclosure is required. U.S. classified material in foreign countries shall be stored at a:

a. U.S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

b. U.S. Government activity located in a building used exclusively by U.S. Government tenants, provided the building is under continuous (i.e., 24/7) control by U.S. Government personnel.

c. U.S. Government activity located in a building not used exclusively by U.S. Government tenants which is under host government control, provided that the classified material is stored in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access and the room or area is under continuous (i.e., 24/7) control by U.S. Government personnel.

d. U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host-government control, provided the classified material is stored in GSA-approved security containers and is placed under continuous (i.e., 24/7) control by U.S. Government personnel.

6. SPECIALIZED STORAGE

a. Military Platforms

(1) The Heads of the DoD Components shall, consistent with this Volume, delineate the appropriate security measures required to protect classified information stored in security containers on military platforms (e.g., aircraft, militarized or tactical vehicle) and for classified munitions items.

(2) GSA-approved field safes and special size one- and two-drawer security containers approved by the GSA may be used for storage of classified information in the field and in military platforms. These containers shall use locks conforming to FF-L-2740 or Federal Specification FF-L-2937 (Reference (am)), as required by Federal Specification AA-F-358 (Reference (an)). Special size containers shall be securely fastened to the platform; field safes shall be under sufficient control and surveillance when in use to prevent unauthorized access or loss.

b. IT Equipment. GSA-approved information processing system cabinets are available for protection of operational IT equipment. The cabinets can be used for storage of network equipment (such as routers, switches, and crypto devices), servers, power control units, and laptops and can be configured for rack mounting with interior fans for heat management and cable connections for exterior data transmission and power.

c. Map and Plan File Cabinets. GSA-approved map and plan file cabinets are available for storing odd-sized items such as computer media, maps, charts, and classified equipment.

d. Modular Vaults. GSA-approved modular vaults meeting Federal Specification AA-V-2737 (Reference (ao)) may be used to store classified information as an alternative to vault requirements described in the Appendix to this enclosure.

e. Bulky Material. Storage areas for bulky material containing Secret or Confidential information may have access openings (e.g., roof hatches, vents) secured by GSA-approved changeable combination padlocks meeting Federal Specification FF-P-110 (Reference (ap)). Other security measures are required, in accordance with paragraphs 3.b. and 3.c. of this enclosure.

(1) When special circumstances exist, the Heads of the DoD Components may authorize the use of key operated locks for storing bulky material containing Secret and Confidential information. The authorization shall be documented with an explanation of the special circumstances that warrant deviation from other established standards. Whenever using such locks, administrative procedures for the control and accounting of keys and locks shall be established. The level of protection provided to such keys shall be equivalent to that afforded the classified information the padlock protects.

(2) Section 1386 of title 18, United States Code (U.S.C.) (Reference (aq)), makes

unauthorized possession of keys, key-blanks, keyways, or locks that any part of the Department of Defense adopts for protecting conventional arms, ammunition, or explosives, special weapons, and classified equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.

7. PROCURING NEW STORAGE EQUIPMENT. New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule. When GSA-approved security containers or vault doors with locks meeting FF-L-2740 are placed in service or when existing mechanical locks are replaced with locks meeting FF-L-2740, the custodian or security manager shall record the lock serial number on an SF 700, "Security Container Information." For procurement or technical support, call the DoD Lock Program as specified in paragraph 1.d of this enclosure.

8. SECURITY CONTAINER LABELS. GSA-approved security containers must have a label stating "General Services Administration Approved Security Container," affixed to the front of the container, usually on the control or the top drawer.

a. If the label is missing or if the container's integrity is in question, the container shall be inspected by a GSA certified inspector. Information on obtaining inspections and recertification of containers can be found on the DoD Lock Program Website (<https://locks.navfac.navy.mil>) or by calling the DoD Lock Program at (800) 290-7607 or DSN 551-1212.

b. When the container is being sent to the Defense Reutilization and Marketing Office, the GSA label shall be removed.

9. EXTERNAL MARKINGS ON CONTAINERS. There shall be no external mark revealing the level of classified information authorized to be or actually stored in a given container or vault, or indicating the priority assigned to the container for emergency evacuation and destruction. This does not preclude placing a mark or symbol (e.g., a bar code) on the container for other purposes (e.g., identification and/or inventory purposes) or from applying decals or stickers the DNI requires for containers and equipment used to store or process intelligence information. If a GSA container or vault door recertification is required, such labels and markings must be removed, but may be reapplied as needed after recertification.

10. SECURITY CONTAINER INFORMATION. Maintain a record for each container, or vault or secure room door, used for storing classified information. SF 700 with all information blocks completed, shall be used for this purpose. Update the form each time the security container combination is changed.

a. Part 1 of SF 700 is not classified, but contains personally identifiable information (PII) that shall be protected by sealing Part 1 in an opaque envelope (not provided as part of the SF 700) conspicuously marked "Security Container Information" and stored in accordance with SF

700 instructions. If the information must be accessed during non-duty hours and a new opaque envelope is not available to replace the opened one, the original envelope should be temporarily resealed, to the extent possible, until Part 1 can be placed in a new envelope the next working day.

b. Part 2 of SF 700, when completed, is classified at the highest level of classification authorized for storage in the security container. It shall be sealed and stored in accordance with SF 700 instructions. The classification authority block shall state "Derived From: 32 CFR 2001.80(d)(3)," with declassification upon change of combination.

11. COMBINATIONS TO CONTAINERS, VAULTS AND SECURE ROOMS

a. Protecting and Storing Combinations. In accordance with section 2001.45(a)(1) of Reference (f), the combination shall be classified at the same level as the highest classification of the material authorized for storage in the container.

(1) Use SF 700 Part 2, as specified in section 10 of this enclosure, to record the combination and other required data.

(2) If another record of the combination is made, the record shall be marked as required by Volume 2 of this Manual.

(3) Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers, including vaults and secure rooms.

(4) Security containers, vaults, secure rooms and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

(5) A record of the names of persons having knowledge of the combination shall be maintained.

b. Changing Combinations. Only individuals with the responsibility and an appropriate security clearance shall change combinations to security containers, vaults and secure rooms used for storing classified information. Combinations shall be changed:

(1) When the container, vault, or secure room door is placed in service.

(2) Whenever an individual knowing the combination to the container or vault door no longer requires access, unless other sufficient controls exist to prevent that individual's access to the lock.

(3) When compromise of the combination is suspected.

(4) When the container, vault, or secure room door is taken out of service or is no longer

used to store classified information, at which time built-in combination locks shall be reset to the standard combination 50-25-50, and combination padlocks shall be reset to the standard combination 10-20-30.

12. ENTRANCES TO OPEN STORAGE AREAS FOR CLASSIFIED INFORMATION

a. When areas storing classified information are occupied by authorized individual(s), the entrances shall either be:

(1) Under visual control at all times to detect entry by unauthorized persons; or

(2) Equipped with an automated entry control system to limit access (see section 3 of the Appendix to this enclosure).

b. Secure rooms or other areas storing classified information shall be secured when the area is not occupied by authorized individual(s) or under continual visual control.

c. The Appendix to this enclosure provides standards for access control devices. Electrically actuated locks (e.g., magnetic strip card locks) do not, by themselves, meet the required standards for protecting classified information and shall not be used as a substitute for the locks prescribed in section 2 of this enclosure.

13. INSPECTION OF STORAGE CONTAINERS PRIOR TO REMOVAL, REPAIR, ETC.

Cleared personnel shall inspect storage containers that may have been used to store classified information before removing them from protected areas or allowing unauthorized persons access to them to ensure no classified material remains within.

14. NEUTRALIZATION AND REPAIR PROCEDURES. The procedures described in FED-STD 809 (Reference (ar)) shall be followed for neutralization and repair of security containers and vault doors. Reference (ar) can be found on the DoD Lock Program Website, <https://locks.navfac.navy.mil>.

a. Neutralization and repair of a security container or door to a vault approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in the methods specified by Reference (ar).

b. Neutralization or repair by, or using, methods and procedures other than described in Reference (ar) is considered a violation of the security container's or vault door's security integrity and the GSA label shall be removed. Thereafter, the containers or doors may not be used to protect classified information.

15. STORAGE OF FGI. To the extent practical, FGI shall be stored separately from other

information to facilitate its control. To avoid additional costs, separate storage may be accomplished by methods such as using separate drawers in the same container as other information or, for small amounts, the use of separate file folders in the same drawer.

16. RETENTION OF CLASSIFIED INFORMATION. Classified documents and other material shall be retained within DoD organizations only if they are required for effective and efficient operation of the organization or if law or regulation requires their retention. Documents no longer required for operational purposes shall be disposed of according to the provisions of chapter 33 of Reference (t) and appropriate implementing directives and records schedules, and in accordance with sections 17 and 18 of this enclosure.

17. DESTRUCTION OF CLASSIFIED INFORMATION. Classified documents and material identified for destruction shall be destroyed completely, to prevent anyone from reconstructing the classified information, according to procedures and methods the DoD Component Head prescribes. Methods and equipment used to routinely destroy classified information include burning, crosscut shredding, wet pulping, mutilation, chemical decomposition or pulverizing. Methods used for clearing, sanitization or destruction of classified IT equipment and media include overwriting, degaussing, sanding, and physical destruction of components or media.

a. Documents and other material identified for destruction shall continue to be protected as appropriate for their classification until actually destroyed.

b. Each activity with classified holdings shall establish at least 1 day each year when specific attention and effort is focused on disposing of unneeded classified material (“clean-out day”).

c. Guidance on standards, processes, and procedures for the destruction of COMSEC and other classified material can be found in Reference (r). NATO material shall be destroyed in accordance with Reference (ac). FGI shall be destroyed in the same manner as U.S. classified information of the equivalent level, except where otherwise required by international treaty or agreement. Also see Enclosure 2, subparagraphs 17.b.(7)(a) through (d) for guidance on recording FGI destruction.

d. Effective January 1, 2011, only equipment listed on an evaluated products list (EPL) issued by NSA may be used to destroy classified information using any method covered by an EPL. EPLs currently exist for paper shredders, punched tape destruction devices, optical media destruction devices (for compact discs (CDs) and digital video discs (DVDs)), degaussers (for magnetic media sanitization), and disintegrators (for paper and punched tape material). The EPLs may be obtained by calling (410) 854-6358 or at http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.

(1) Equipment approved for use prior to January 1, 2011, and not found on the appropriate EPL may be used for destruction of classified information until December 31, 2016.

(2) Unless determined otherwise by NSA, whenever an EPL is revised, equipment

removed from the EPL may be utilized for destruction of classified information for up to 6 years from the date of its removal from the EPL.

(3) In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly (e.g., shredder blade assembly), the unit must be replaced with one listed on the appropriate EPL.

e. Classified IT storage media (e.g., hard drives) cannot be declassified by overwriting. Sanitization (which may destroy the usefulness of the media) or physical destruction is required for disposal. See also section 6 of Enclosure 7 of this Volume.

18. TECHNICAL GUIDANCE ON DESTRUCTION METHODS. Contact the National Security Agency/Central Security Service (NSA/CSS) System and Network Analysis Center at (410) 854-6358 or via e-mail at SNAC@radium.ncsc.mil, to obtain technical guidance concerning appropriate methods, equipment, and standards for destroying classified electronic media, IT equipment, electronic components, and other similar or associated materials.

a. Crosscut Shredders. Only crosscut shredders listed on the “NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders” (Reference (as)) may be used to destroy classified material by shredding.

(1) The EPL is updated on an as-needed basis as new models are successfully evaluated. Users are encouraged to contact shredders manufacturers and/or distributors for assistance in selecting unit(s) best suited to their requirements. Vendors and/or distributors can provide guidance on whether a specific model not listed meets the specifications in Reference (as) (e.g., for shred size) and, as applicable, a copy of the NSA/CSS letter confirming that the model will be included on the EPL at its next update.

(2) Crosscut shredders currently in use and not on the EPL that were at the time of acquisition on a NSA/CSS evaluated approved products list as being capable of maintaining a shred size of 1/2 inch by 1/32 inch (variance of 1/64 inch) may be used until December 31, 2016 in accordance with paragraph 17.d of this enclosure, EXCEPT for destruction of COMSEC materials. However, any such crosscut shredders requiring replacement of the unit and/or rebuild of the shredder blades assembly MUST BE REPLACED by a crosscut shredder on the latest NSA/CSS EPL. When COMSEC material is destroyed by shredding, ONLY crosscut shredders listed in Reference (as) at the time of acquisition shall be used.

(a) Pending replacement, the Heads of DoD Components shall ensure that procedures are in place to manage the risk posed by crosscut shredders not on the approved NSA/CSS list. At a minimum, the volume and content of each activity’s classified material destruction flow shall be assessed and a process established to optimize the use of high security crosscut paper shredders (i.e., with top secret collateral material being the highest collateral priority) to take full advantage of the added security value of those shredders.

(b) The bag of shred must be “stirred” to ensure that the content is mixed up.

(c) Shredding of unclassified material along with the classified material is encouraged.

b. Pulverizers and Disintegrators. Pulverizers and disintegrators must have a 3/32 inch or smaller security screen. Consult the “NSA/CSS Evaluated Products List for High Security Disintegrators” (Reference (at)) for additional details and guidance.

c. Pulping. Pulping (wet process) devices with a 1/4 inch or smaller security screen may be used to destroy classified water-soluble material.

19. DESTRUCTION PROCEDURES

a. The Heads of the DoD Component shall establish procedures to ensure that all classified information intended for destruction is destroyed by authorized means and appropriately cleared personnel.

b. Classified information that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to a designated record center.

c. Classified information shall be controlled in a manner designed to minimize the possibility of unauthorized removal and/or access. A burn bag may be used to store classified information awaiting destruction at a central destruction facility. Seal and safeguard each burn bag per this Volume until actually destroyed.

d. Records of destruction are not required, except as noted in paragraph 17.c of this enclosure and, for destruction of classified FGI, in Enclosure 2, subparagraphs 17.b.(7)(a) through (d).

Appendix

Physical Security Standards

APPENDIX TO ENCLOSURE 3

PHYSICAL SECURITY STANDARDS

1. VAULT AND SECURE ROOM CONSTRUCTION STANDARDS

a. Vaults. Vaults shall be constructed to meet Reference (al) as follows:

- (1) Class A (concrete poured-in-place).
- (2) Class B (GSA-approved modular vault meeting Reference (ao) specifications).
- (3) Class C (steel-lined vault) is NOT authorized for protection of classified information.

b. Open Storage Area (Secure Room). This section provides the minimum construction standards for open storage areas.

(1) Walls, Floor, and Roof. Walls, floor, and roof shall be of permanent construction materials; i.e., plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to and evidence of unauthorized entry into the area. Walls shall be extended from the true floor to the true ceiling and attached with permanent construction materials, mesh, or 18 gauge expanded steel screen.

(2) Ceiling. The ceiling shall be constructed of plaster, gypsum, wallboard material, hardware or any other acceptable material.

(3) Doors. Access doors shall be substantially constructed of wood or metal. For out-swing doors, hinge-side protection shall be provided by making hinge pins non-removable (e.g., spot welding) or by using hinges with interlocking leaves that prevent removal. Doors shall be equipped with a GSA-approved combination lock meeting FF-L-2740. Doors other than those secured with locks meeting FF-L-2740 shall be secured from the inside with deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar that extends across the width of the door.

(4) Windows

(a) Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects located directly beneath the windows, shall be constructed from or covered with materials that will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Secure rooms which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by motion detection sensors within the area).

(b) Windows, which might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings.

(5) Utility Openings. Utility openings such as ducts and vents shall be smaller than man-passable (96 square inches). An opening larger than 96 square inches (and over 6 inches in its smallest dimension) that enters or passes through an open storage area shall be hardened in accordance with Military Handbook 1013/1A (Reference (au)).

2. IDS STANDARDS

a. IDS Purpose. An IDS shall detect an unauthorized penetration into the secured area. An IDS shall be installed when results of a documented risk assessment determine its use as a supplemental control is warranted, in accordance with Enclosure 3, sections 3 and 4 of this Volume, and use is approved by the activity head. When used, all areas that reasonably afford access to the security container or areas where classified data is stored shall be protected by IDS unless continually occupied. An IDS complements other physical security measures and consists of:

- (1) Intrusion detection equipment (IDE).
- (2) Security forces.
- (3) Operating procedures.

b. System Functions

- (1) IDS components operate as a system with four distinct phases:
 - (a) Detection.
 - (b) Communications.
 - (c) Assessment.
 - (d) Response.
- (2) These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.

(a) Detection. During the detection phase, a detector or sensor senses and reacts to the stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area to the premise control unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise a zone at the monitor station (i.e., an

alarmed zone).

(b) Communications. The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. An additional signal is added to the communication for supervision to prevent compromise of the communication scheme (i.e., tampering or injection of false information by an intruder). The supervised signal is sent by the PCU through the transmission link to the monitor station. Inside the monitor station either a dedicated panel or central processor monitors information from the PCU signals. When an alarm occurs, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

(c) Assessment. The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force.

(d) Response. The response phase begins as soon as the operator assesses an alarm condition. A response force shall immediately respond to all alarms. The response phase shall also determine the precise nature of the alarm and take all measures necessary to safeguard the secure area.

c. Acceptability of Equipment: All IDE must be Underwriters Laboratories (UL)-listed (or equivalent) and approved by the DoD Component. Government installed, maintained, or furnished systems are acceptable.

d. Transmission and Annunciation

(1) Transmission Line Security. When the transmission line leaves the facility and traverses an uncontrolled area, Class I or Class II line supervision shall be used.

(a) Class I. Class I security is achieved through the use of Data Encryption Standard or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by the National Institutes of Standards and Technology or another independent testing laboratory is required.

(b) Class II. Class II line supervision refers to systems in which the transmission is based on pseudo-random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum 6-month period. Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

(2) Internal Cabling. The cabling between the sensors and the PCU shall be dedicated to IDE and shall comply with national and local code standards.

(3) Entry and/or Access Control Systems. If an entry and/or access control system is integrated into an IDS, reports from the automated entry and/or access control system shall be subordinate in priority to reports from intrusion alarms.

(4) Maintenance Mode. When the alarm zone is placed in the maintenance mode, this condition shall be signaled automatically to the monitor station. The signal shall appear as an alarm or maintenance message at the monitor station and the IDS shall not be securable while in the maintenance mode. The alarm or message shall be continually visible at the monitor station throughout the period of maintenance. A standard operating procedure shall be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods shall be archived in the system. A self-test feature shall be limited to one second per occurrence.

(5) Annunciation of Shunting or Masking Condition. Shunting or masking of any internal zone or sensor shall be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor shall be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

(6) Indications of Alarm Status. Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the secure area.

(7) Power Supplies. Primary power for all IDE shall be commercial alternating or direct current (AC or DC) power. In the event of commercial power failure at the protected area or monitor station, the equipment shall change power sources without causing an alarm indication.

(a) Emergency Power. Emergency power shall consist of a protected independent backup power source that provides a minimum of 8 hours operating power battery and/or generator power. When batteries are used for emergency power, they shall be maintained at full charge by automatic charging circuits. The manufacturer's periodic maintenance schedule shall be followed and results documented.

(b) Power Source and Failure Indication. An illuminated indication shall exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station shall indicate a failure in power source, a change in power source, and the location of the failure or change.

(8) Component Tamper Protection. IDE components located inside or outside the secure area shall be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection shall be provided.

e. System Requirements

(1) Independent Equipment. When many alarmed areas are protected by one monitor station, secure room zones shall be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

(2) Access and/or Secure Switch and PCU. No capability shall exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs shall be located inside the secure area and should be located near the entrance. Assigned personnel shall initiate all changes in access and secure status. Operations of the PCU may be restricted by use of a

device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

(3) Motion Detection Protection. Secure areas that reasonably afford access to the security container or area where classified data is stored shall be protected with motion detection sensors; e.g., ultrasonic and passive infrared. Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector shall cause an immediate and continuous alarm condition.

(4) Protection of Perimeter Doors. When an IDS is installed, each perimeter door shall be protected by a balanced magnetic switch that meets UL Standard 634 (Reference (av)).

(5) Windows. All readily accessible windows (within 18 feet of ground level) shall be protected by an IDS, either independently or by the motion detection sensors within the space, whenever a secure room is located within a controlled compound or equivalent and forced entry protection of the windows is not provided (also see subparagraph 1.b.(4) of this Appendix).

(6) IDS Requirements for Continuous Operations Facilities. A continuous operation facility may not require an IDS. This type of secure area should be equipped with an alerting system if the occupants cannot observe all potential entrances into the room. Duress devices may also be required.

(7) False and/or Nuisance Alarm. Any alarm signal transmitted in the absence of detected intrusion that is not identified as a nuisance alarm is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. All alarms shall be investigated and the results documented. The maintenance program for the IDS shall ensure that incidents of false and/or nuisance alarms shall not exceed 1 in a period of 30 days per zone.

f. Installation, Maintenance and Monitoring

(1) IDS Installation and Maintenance Personnel. Alarm installation and maintenance shall be accomplished by U.S. citizens who have been subjected to a trustworthiness determination according to Reference (1).

(2) Monitor Station Staffing. The monitor station shall be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination according to Reference (1).

3. ACCESS CONTROLS

a. The perimeter entrance to a secure facility (i.e., vault or secure room) shall be under control at all times during working hours to prevent entry by unauthorized personnel. This may be achieved by visual control or through use of an automated entry control system (AECS) that complies with the requirements of subparagraph 3.a.(2) of this section. Uncleared persons are to

be escorted within the facility by a cleared person who is familiar with the security procedures of the facility. Personnel entering or leaving an area shall be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirming their need to know and access.

(1) Visual control may be accomplished by methods such as designated employees, guards, or continuously monitored closed circuit television.

(2) An AECS may be used if it meets the criteria stated in subparagraphs 3.a.(2)(a) and 3.a.(2)(b). The AECS shall identify an individual and authenticate the person's authority to enter the area through the use of an identification (ID) badge or card.

(a) The ID badge or key card shall use embedded sensors, integrated circuits, magnetic stripes, or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(b) Biometrics verification identifies the individual requesting access by some unique personal characteristic and may be required for access to sensitive information. The Biometrics Identity Management Agency can provide further information regarding biometric technologies and capabilities. Personal characteristics that can be used for identity verification include:

1. Fingerprints.
2. Hand geometry.
3. Handwriting.
4. Iris scans.
5. Voice.
6. Facial recognition.

(3) In conjunction with subparagraph 3.a.(2)(a) of this section, a personal identification number (PIN) may be required. The PIN shall be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN shall be changed when it is believed to have been compromised or subjected to compromise.

(4) Authentication of the individual's authorization to enter the area shall be accomplished within the system by inputs from the ID badge and/or card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. A procedure shall be established for removing the individual's authorization to enter the area upon reassignment, transfer, or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than the required access level.

(5) Protection shall be established and maintained for all devices or equipment that constitutes the entry control system. The level of protection may vary depending upon the type of device or equipment being protected.

(a) Location where authorization data and personal identification or verification data is input, stored, or recorded shall be protected.

(b) Card readers, keypads, communication or interface devices located outside the entrance to a controlled area shall have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.

(c) Keypad devices shall be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

(d) Systems that use transmission lines to carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area shall have line supervision.

(e) Electric strikes used in access control systems shall be heavy duty, industrial grade.

(6) Access to records and information concerning encoded identification data and PINs shall be restricted. Access to identification or authorizing data, operating system software or any identifying data associated with the entry control system shall be limited to the fewest number of personnel as possible. Such data or software shall be kept secure when unattended.

(7) Records shall be maintained reflecting active assignment of identification badge and/or card, PIN, level of access, and similar system-related records. Records concerning personnel removed from the system shall be retained for at least 90 days. Records of entries shall be retained for at least 90 days or until investigations of system violations and incidents have been resolved and recorded. Such records shall be destroyed when no longer required in accordance with Reference (u) and DoD Component implementing directives and records schedules.

b. The Heads of DoD Components may approve the use of standardized AECS that meet the following criteria:

(1) For a Level 1 key card system, i.e., a key card bearing a magnetic stripe, the AECS shall provide a .95 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system shall ensure an unauthorized user is granted access with less than 0.05 probability after three attempts to gain entry.

(2) For a Level 2 key card and PIN system, i.e., a key card bearing a magnetic stripe

used in conjunction with a PIN, the AECS shall provide a 0.97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an unauthorized user is granted access with less than 0.010 probability after three attempts to gain entry have been made.

(3) For a Level 3 key card, i.e., a key card bearing a magnetic stripe used in conjunction with a PIN and biometrics identifier system, the AECS shall provide a 0.97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system shall ensure an unauthorized user is granted access with less than 0.005 probability after three attempts to gain entry have been made.

c. Electrical, mechanical, or electromechanical access control devices meeting the criteria stated below, may be used to control access to secure areas during duty hours if the entrance is under visual control. These devices are also acceptable to control access to compartmented areas within a secure area. Access control devices shall be installed in the following manner:

(1) The electronic control panel containing the mechanism for setting the combination shall be located inside the area. The control panel shall require only a minimal degree of physical security designed to preclude unauthorized access to the mechanism.

(2) The control panel shall be installed, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.

(3) An individual cleared at the same level as the highest classified information controlled within the area shall select and set the combination.

(4) Electrical components, including wiring, or mechanical links (cables, rods, and so on) shall be accessible only from inside the area, or, if they traverse an uncontrolled area, they shall be secured within conduit to preclude surreptitious manipulation of components.

ENCLOSURE 4

TRANSMISSION AND TRANSPORTATION

1. TRANSMISSION AND TRANSPORTATION PROCEDURES. Heads of the DoD Components shall establish procedures for transmitting and transporting classified information that maximizes the accessibility of classified information to individuals who are eligible for access thereto and minimizes the risk of compromise while permitting the use of the most cost-effective means. Persons transmitting or transporting classified information are responsible for ensuring that the intended recipient(s) are authorized access, have a need to know, and have the capability to store classified information in accordance with the requirements of this Manual.

a. COMSEC information shall be transmitted and transported according to NSA/CSS Policy Manual 3-16 (Reference (aw)).

b. NATO classified information, including NATO Restricted, shall be transmitted according to the requirements of Reference (ac).

2. DISSEMINATION OUTSIDE THE DEPARTMENT OF DEFENSE

a. Classified information originating in another DoD Component or in a department or agency other than the Department of Defense may be disseminated to other DoD Components, to other U.S. departments or agencies, or to a U.S. entity without the consent of the originating Component, department, or agency, as long as:

(1) The criteria for access in section 3 of Enclosure 2 of this Volume are met.

(2) The classified information is NOT marked as requiring prior authorization for dissemination to another department or agency. The marking "ORCON" may be used to identify information requiring prior authorization for dissemination to another department or agency.

(3) The document was created ON or AFTER June 27, 2010, the effective date of Reference (f) (however, also see paragraph 2.b of this section).

b. Documents created BEFORE June 27, 2010 may not be disseminated outside of the Department of Defense without the originator's consent. Additionally, documents created on or after June 27, 2010, whose classification is derived from documents created prior to that date, and where the date before June 27, 2010 of the classified source(s) is readily apparent from the source list, shall not be disseminated outside of the Department of Defense without the originator's consent.

c. Classified information originating in, or provided to or by, the Department of Defense may be disseminated to a foreign government or an international organization of governments, or any element thereof, in accordance with References (d), (f) and (z). See section 6 of this

enclosure for further guidance.

d. Dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued by the DNI.

e. Dissemination of classified information to state, local, tribal and private sector officials pursuant to E.O. 13549 (Reference (ax)) shall be in accordance with implementing guidance issued by the Department of Homeland Security.

3. TRANSMISSION OF TOP SECRET INFORMATION. Top Secret information shall be transmitted only by:

a. Direct contact between appropriately cleared persons.

b. Electronic means over an approved secure communications system (i.e., a cryptographic system authorized by the Director, NSA, or a protected distribution system designed and installed to meet the requirements of National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003 (Reference (ay))). This applies to voice, data, message (both organizational and e-mail), and facsimile transmissions.

c. The Defense Courier Service (DCS) if the material qualifies under the provisions of DoDI 5200.33 (Reference (az)). The DCS may use a specialized shipping container as a substitute for a DCS courier on direct flights if the shipping container is sufficiently constructed to provide evidence of forced entry, secured with a high security padlock meeting Reference (ap) specifications and equipped with an electronic seal that would provide evidence of surreptitious entry. A DCS courier shall escort the specialized shipping container to and from the aircraft and oversee its loading and unloading. This authorization also requires that the DCS develop procedures that address protecting specialized shipping containers in the event a flight is diverted for any reason.

d. Authorized U.S. Government agency courier services (e.g., Department of State Diplomatic Courier Service, authorized DoD Component courier service).

e. Appropriately cleared U.S. Military and Government civilian personnel specifically designated to carry the information and traveling by surface transportation.

f. Appropriately cleared U.S. Military and Government civilian personnel specifically designated to carry the information and traveling on scheduled commercial passenger aircraft within and between the United States, its territories, and Canada.

g. Appropriately cleared U.S. Military and Government civilian personnel specifically designated to carry the information and traveling on scheduled commercial passenger aircraft on flights outside the United States, its territories, and Canada.

h. DoD contractor employees with appropriate clearances traveling within and between the

United States and its territories provided the requirements of Reference (x) and DoD 5220.22-R (Reference (ba)) are met.

4. TRANSMISSION OF SECRET INFORMATION. Secret information may be transmitted by:

a. Any of the means approved for the transmission of Top Secret information.

b. Appropriately cleared contractor employees if the transmission meets the requirements specified in References (x) and (ba).

c. Overnight delivery, provided the requirements of this paragraph are met. Heads of DoD Components may, when a requirement exists for overnight delivery to a DoD Component within the United States and its territories, authorize the use of the current holder of the GSA contract for overnight delivery of information for the Executive Branch as long as applicable postal regulations (chapter I of title 39, CFR (Reference(bb))) are met. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract shall require cooperation with U.S. Government inquiries in the event of a loss, theft, or possible compromise. The sender is responsible for ensuring that an authorized person at the receiving end is aware that the package is coming and will be available to receive the package, verifying the mailing address is correct, and confirming (by telephone or e-mail) that the package did in fact arrive within the specified time period. The package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified COMSEC information, NATO information, SCI, and FGI shall not be transmitted in this manner. See Multiple Award Schedule 48, "Transportation, Delivery and Relocation Solutions," on the GSA eLibrary Website (<http://www.gsaelibrary.gsa.gov/ElibMain/home.do>) for a listing of commercial carriers authorized for use under the provisions of this paragraph.

d. U.S. Postal Service registered mail within and between the United States, the District of Columbia, and the Commonwealth of Puerto Rico.

e. U.S. Postal Service Express mail within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico. The "Waiver of Signature and Indemnity" block on the U.S. Postal Service Express Mail Label 11-B may not be executed under any circumstances. The use of external (street side) Express Mail collection boxes is prohibited.

f. U.S. Postal Service and Canadian registered mail with registered mail receipt between U.S. Government and Canadian government installations in the United States and Canada.

g. U.S. Postal Service registered mail through Military Postal Service facilities outside the United States and its territories, if the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection.

h. Carriers cleared under the National Industrial Security Program providing a protective security service. This method is authorized only within the continental United States (CONUS) when other methods are impractical, except that this method is also authorized between U.S. and Canadian government approved locations documented in a transportation plan approved by U.S. and Canadian government security authorities.

i. U.S. Government and U.S. Government contract vehicles including aircraft, ships of the U.S. Navy, civil service-operated U.S. Naval ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are U.S. citizens may be designated as escorts provided the control of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. Observing the shipment is not required during flight or sea transit, provided it is loaded into a compartment that is not accessible to any unauthorized persons or in a specialized secure, safe-like container.

j. Air carrier without an appropriately cleared escort to locations outside the United States and its territories, provided the provisions of this paragraph are met. In exceptional circumstances, with the written approval of the sending and receiving government DSAs, material may be transmitted outside the United States and its territories without an appropriately cleared escort provided the following criteria are met:

(1) The material is stored in the hold of an aircraft of an U.S. owned or registered air carrier or an air carrier owned by or under the registry of the recipient government.

(2) The shipment is placed in a compartment that is not accessible to any unauthorized person or in a specialized shipping container approved for this purpose.

(3) The air carrier agrees in writing to permit a cleared DoD or cleared U.S. company employee, specifically designated by name, to observe placement of the classified shipment into the aircraft.

(4) The flight is direct between two designated points with no intermediate stops.

(5) The air carrier agrees in writing that a designated officer on the aircraft will assume responsibility for the classified material while en route to the destination.

(6) Written emergency instructions are provided to the air carrier.

(7) Arrangements are made for recipient foreign government officials, the designated government representative (DGR), or other recipient government representative, designated by name and organization, in writing, to be present at the unloading of the consignment and immediately assume security control for the recipient government.

(8) The foregoing requirements are documented in the transportation plan.

(9) The exceptional circumstances are documented in the request for exception.

5. TRANSMISSION OF CONFIDENTIAL INFORMATION. Confidential information may be transmitted by:

a. Any of the means approved for the transmission of Secret information.

b. U.S. Postal Service Registered Mail for:

(1) Material to and from military post office addressees (i.e., Fleet Post Office or Army Post Office) located outside the United States and its territories.

(2) Material when the originator is uncertain that the addressee's location is within U.S. boundaries.

c. U.S. Postal Service certified mail (or registered mail, if required above) for material addressed to DoD contractors or non-DoD agencies.

d. U.S. Postal Service first class mail between DoD Component locations anywhere in the United States and its territories. The outer envelope or wrapper shall be endorsed: "Return Service Requested."

e. Commercial carriers that provide a constant surveillance service, as defined in Reference (x), within CONUS.

f. Commanders or masters of ships of U.S. registry who are U.S. citizens. Confidential information shipped on ships of U.S. registry may not pass out of U.S. Government control. The commanders or masters shall sign a receipt for the material and agree to:

(1) Deny unauthorized persons access to the Confidential material, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection shall not be unloaded.

(2) Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

g. Alternative or additional methods of transmission the Head of the DoD Component approves.

6. TRANSMISSION OF CLASSIFIED INFORMATION AND MATERIAL TO FOREIGN GOVERNMENTS. Classified information and material approved for release to a foreign government or international organization (collectively "foreign governments") according to Reference (z) shall be transmitted between representatives of each government through government-to-government channels or through other channels agreed to in writing by the DSAs of the sending and receiving governments. International transfers of classified material shall

comply with this enclosure, its appendix, and the following:

a. U.S. Government control and accountability of classified information or material shall be maintained from the point of origin to the ultimate destination, until it is officially transferred to the intended recipient government through its designated government representative (DGR).

b. In urgent situations, appropriately cleared U.S. Government agency employees may be authorized to hand-carry classified material in accordance with this enclosure and its appendix.

c. Each DoD Component entering into a contract or an international agreement that will entail the transfer of classified information and material to a foreign government shall consult with supporting DoD transportation and security authorities to confirm the appropriate transfer arrangements and establish responsibilities for the transfer arrangements prior to the execution of the agreement or contract.

7. SECURITY REQUIREMENTS FOR TRANSFERS OF DEFENSE ARTICLES TO AUSTRALIA OR THE UNITED KINGDOM WITHOUT AN EXPORT LICENSE OR OTHER WRITTEN AUTHORIZATION

a. Background. The Defense Trade Cooperation Treaty between the United States and Australia, which was signed by the United States on September 5, 2007, and the Defense Trade Cooperation Treaty between the United States and the United Kingdom (UK), which was signed by the United States on June 21, 2007, provide comprehensive frameworks for exports and transfers of certain classified and unclassified defense articles, without an export license or other written authorization to Australian Communities and United Kingdom Communities respectively (see Glossary). The provisions of the treaties apply to both government organizations and contractors. This section provides implementing guidance to DoD entities that are eligible to export certain classified and unclassified defense articles.

b. Applicability. Defense articles (defined in Glossary) fall under the scope of the treaties when they are in support of:

- (1) United States and Australia or UK, as applicable, combined military or counter-terrorism operations;
- (2) United States and Australia or UK, as applicable, cooperative security and defense research, development, production, and support programs;
- (3) Mutually determined specific security and defense projects where the Government of Australia or Government of the United Kingdom, as applicable, is the end-user; or
- (4) U.S. Government end-use.

c. Markings. Prior to transfer to Australia or the UK, defense articles that fall under the scope of these treaties must be labeled, as applicable, with an overall marking as directed in

subparagraph 7.c.(1) or 7.c.(2) of this enclosure. While these markings do not generally conform to the marking standard specified in Volume 2 of this Manual, the markings are required by these Defense Trade Cooperation Treaties and their Implementing Arrangements and must be used as specified.

(1) Markings required for transfer of defense articles to Australia:

(a) Classified U.S. defense articles shall be marked:

CLASSIFICATION LEVEL USML//REL AUS AND USA TREATY COMMUNITY//

For example, for defense articles classified SECRET, the marking shall be “SECRET USML//REL AUS AND USA TREATY COMMUNITY//.” Apply other applicable classification markings (e.g., classification authority block, portion markings, other dissemination markings) in accordance with Volume 2 of this Manual.

(b) Unclassified U.S. defense articles shall be marked:

//RESTRICTED USML//REL AUS AND USA TREATY COMMUNITY//

(c) When defense articles are returned from Australia to the United States, any defense articles marked as RESTRICTED in this manner purely for the purposes of the treaty will be considered to be unclassified and such markings shall be removed.

(2) Markings required for transfer of defense articles to the UK:

(a) Classified U.S. defense articles shall be marked:

CLASSIFICATION LEVEL USML//REL USA AND GBR TREATY COMMUNITY//

For example, for defense articles classified SECRET, the marking shall be “SECRET USML//REL USA AND GBR TREATY COMMUNITY//.” Apply other applicable classification markings (e.g., classification authority block, portion markings, other dissemination markings) in accordance with Volume 2 of this Manual.

(b) Unclassified U.S. defense articles shall be marked:

//RESTRICTED USML//REL USA AND GBR TREATY COMMUNITY//

(c) When defense articles are returned from the UK to the United States, any defense articles marked as RESTRICTED in this manner purely for the purposes of the treaty will be considered to be unclassified and such marking shall be removed.

(3) The following notice shall be included (e.g., as part of the bill of lading) whenever defense articles are exported in accordance with the provisions of these treaties: “These U.S. Munitions List commodities are authorized by the U.S. Government under the U.S.-[Australia or

United Kingdom, as applicable] Defense Trade Cooperation Treaty for export only to [Australia or United Kingdom, as applicable] for use in approved projects, programs or operations by members of the [Australian or United Kingdom, as applicable] Community. They may not be retransferred or reexported or used outside of an approved project, program, or operation, either in their original form or after being incorporated into other end-items, without the prior written approval of the U.S. Department of State.”

(4) The items to be marked are:

(a) Defense articles (other than technical data) shall be individually labeled with the appropriate marking detailed in paragraphs 7.c.(1) or 7.c.(2) of this section; or, where such labeling is impracticable (e.g., propellants, chemicals), shall be accompanied by documentation clearly associating the defense articles with the appropriate markings as detailed in paragraphs 7.c.(1) or 7.c.(2) of this section.

(b) Technical data (including technical papers, manuals, presentations, specifications, guides and reports), regardless of media or means of transmission (physical, oral, or electronic), shall be individually labeled with the appropriate marking detailed in paragraphs 7.c.(1) or 7.c.(2) of this section; or, where such labeling is impracticable shall be accompanied by documentation or verbal notification clearly associating the technical data with the appropriate markings as detailed in paragraphs 7.c.(1) or 7.c.(2) of this section.

d. Transfers

(1) All defense articles that fall under the scope of the treaty must be transferred from the U.S. point of embarkation through channels approved by both the United States and, as appropriate, Australia or the UK.

(2) For transfers of defense articles as freight, the contractor shall prepare a transportation plan in accordance with section 10 of the Appendix to Enclosure 4 of this Volume. For transfer of classified U.S. defense articles, a freight forwarder must have a valid facility security clearance and storage capability at the appropriate level. For unclassified U.S. defense articles that are transferred as freight, a freight forwarder is not required to be cleared.

8. USE OF SECURE COMMUNICATIONS FOR TRANSMISSION OF CLASSIFIED INFORMATION. Transmission of DoD information shall comply, as appropriate, with the COMSEC measures and procedures identified in DoDI 8523.01 (Reference (bc)).

a. Computer-to-Computer Transmission. In addition to meeting the requirements of paragraph 3.b of this enclosure, computer and other IT systems used for transmitting classified information shall be approved and accredited in accordance with Reference (s) or Intelligence Community Directive 503 (Reference (bd)), as applicable, to operate at a level of classification commensurate with the data being transmitted. Electronic transmission of classified information over secure computer-to-computer links (e.g., via secure e-mail) is preferable to physical transfer of hard copy documents. Classified information transmitted in this manner shall be marked in

accordance with Volume 2 of this Manual.

b. Facsimile (Fax) Transmission. Only secure facsimile equipment shall be used for facsimile transmission of classified information. The following procedures shall be followed:

(1) The individual transmitting the information shall ensure the recipient has the appropriate clearance and a need to know, and that the secure connection is at the appropriate level of classification for the information being transmitted.

(2) Header or cover sheets used to precede the transmission of classified material shall be conspicuously marked with the highest security classification of the transmitted information and any required control markings. The cover sheet shall also include the originator's name, organization, phone number, an unclassified title, the number of pages, and the receiver's name, organization and phone number. When the cover sheet contains no classified information, it shall also note "Unclassified When Classified Attachment(s) Removed."

(3) Documents transmitted by fax shall have all markings required for a finished document, and shall be controlled and safeguarded by the recipient accordingly.

c. Telephone. Only approved secure telephones, including cell phones and phones integral to personal electronic devices, authorized by the Director, NSA pursuant to paragraph 3.b of this enclosure, may be used for telephonic transmission of classified information. Users must ensure the secure connection is at the appropriate level of classification for the information being discussed.

9. SHIPMENT OF BULK CLASSIFIED MATERIAL AS FREIGHT. Procedures established for shipping bulk classified material as freight shall include provisions for shipping material in closed vehicles when required, appropriate notice to the consignee concerning the shipment, procedures at transshipment activities, and actions to be taken in the case of non-delivery or unexpected delay in delivery.

10. PREPARATION OF MATERIAL FOR SHIPMENT. When transferring classified information, it shall be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and facilitate detection of tampering.

a. Prepare, package, and securely seal classified material in ways that minimize risk of accidental exposure or undetected deliberate compromise. To minimize the risk of exposure of classified information, package documents so that classified material is not in direct contact with the inner envelope or container (e.g., fold so classified material faces together).

(1) Address the outer envelope or container to an official U.S. Government activity or to a DoD contractor with a facility clearance and appropriate storage capability and show the complete return address of the sender. Do not address the outer envelope to an individual. Office codes or phrases such as "Attention: Research Department" may be used.

(2) Show the address of the receiving activity, the address of the sender, the highest classification of the contents (including, where appropriate, any special dissemination or control markings such as “Restricted Data” or “NATO”), and any applicable special instructions on the inner envelope or container. The inner envelope may have an attention line with a person’s name.

(3) Do not place a classification marking or any other unusual marks on the outer envelope or container that might invite special attention to the fact that the contents are classified.

(4) Address classified information intended only for U.S. elements of international staffs or other organizations specifically to those elements.

b. When classified material is hand-carried outside an activity, a locked briefcase or zippered pouch may serve as the outer wrapper. In such cases, the addressing requirements of subparagraph 10.a.(1) of this section do not apply. Refer to section 11 of this enclosure for additional requirements on use of briefcases and pouches.

c. If the classified material is an accessible internal component of an item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information.

d. If the classified material is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered a sufficient enclosure provided observation of it does not reveal classified information.

e. If the classified material is an item of equipment that cannot be packaged and the shell or body is classified, it shall be concealed with an opaque covering hiding all classified features.

f. Specialized shipping containers, including closed cargo transporters, may be considered the outer wrapping or cover.

11. USE OF BRIEFCASES OR ZIPPERED POUCHES FOR HAND-CARRYING

CLASSIFIED MATERIAL. A locked briefcase or zippered pouch made of canvas or other heavy-duty material and having an integral key-operated lock may be used for hand-carrying classified material outside an activity. Such cases may also be used to restrict access to classified material when the intended recipient is not immediately available. If using a briefcase or pouch to hand-carry classified material outside an activity, or in any circumstance when the possibility exists that the briefcase or pouch shall be left for subsequent opening by the intended recipient, package the material as required by section 10 of this enclosure and additionally observe the following procedures:

a. Clearly and recognizably display the name and street address of the organization sending the classified material, and the name and telephone number of a point of contact within the

sending activity, on the outside of the briefcase or pouch.

b. Serially number the pouch or briefcase and clearly display this serial number on its exterior surface.

c. Lock the briefcase or pouch and place its key in a separate sealed envelope.

d. Store the briefcase or pouch, when containing classified material, according to the highest classification level and any special controls applicable to its contents.

e. Ensure the activity authorizing use of the briefcase or pouch maintains an internal system to account for and track the location of the pouch and its key.

f. Use a briefcase or pouch only to assist in enforcing need to know. Its use shall in no way abrogate personal responsibility to ensure that the classified material is delivered to a person who has an appropriate security clearance and access for the information involved.

12. ESCORT, COURIER, OR HAND-CARRY OF CLASSIFIED MATERIAL

a. Authority. Appropriately cleared and briefed personnel may be authorized to escort or carry classified material between locations when other means of transmission or transportation cannot be used. The Heads of the DoD Components shall establish procedures to ensure that hand-carrying of classified material is minimized to the greatest extent possible and does not pose unacceptable risk to the information. Hand carrying may be authorized only when:

(1) The information is not available at the destination and operational necessity or a contractual requirement requires it.

(2) The information cannot be sent via a secure e-mail, facsimile transmission or other secure means.

(3) The appropriate official authorizes the hand-carry according to procedures the Head of the DoD Component establishes.

(4) The hand-carry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, and the U.S. escort retains custody and physical control of the information at all times.

(5) Arrangements have been made for secure storage of the information at a U.S. Government or cleared U.S. contractor facility.

b. Packaging Requirements. Classified material that is hand-carried shall be packaged in the same manner as described in section 10 of this enclosure for material being shipped.

c. Responsibilities. Individuals hand carrying or serving as couriers or escorts for classified information shall be informed of, and acknowledge, their security responsibilities. These requirements may be satisfied by a briefing or by requiring the individual to read written instructions that state the following responsibilities:

- (1) The individual is liable and responsible for the material being carried or escorted.
- (2) The material is not, under any circumstances, to be left unattended. During overnight stops arrangements shall be made for storage of the classified material at a U.S. military facility, embassy, or cleared contractor facility. Classified information shall not be stored in hotel safes.
- (3) The material shall not be opened en route except in the circumstances described in paragraph 12.d of this section.
- (4) The material shall not be discussed or disclosed in any public place.
- (5) The individual shall not deviate from the authorized travel schedule.
- (6) In cases of emergency, the individual shall take measures to protect the material.
- (7) The individual is responsible for ensuring that personal travel documents (passport, courier authorization (if required), medical documents, etc.) are complete, valid, and current.

d. Customs, Police, and Immigration. Arrangements shall be made in advance with customs, police and/or immigration officials to facilitate movement through security. However, there is no assurance of immunity from search by the customs, police, and/or immigration officials of countries, including the United States, whose border the courier may cross. Therefore, if such officials inquire into the contents of the consignment, the courier shall present the courier authorization or orders and ask to speak to the senior customs, police, and/or immigration official. This action shall normally suffice to pass the material through unopened. However, if the senior official demands to see the actual contents of the package, it may be opened in his or her presence, but shall be done in an area out of sight of the public. In that instance:

- (1) Precautions shall be taken to show officials only as much of the contents as satisfies them that the package does not contain any other item. The courier shall ask the official to repack the material or assist in repacking it immediately upon completing the examination.
- (2) The senior customs, police, or immigration official shall be requested to provide evidence of opening and inspection of the package by sealing and signing it when closed and confirming on the shipping documents (if any) or courier certificate that the package has been opened. Both the addressee and the dispatching security officer shall be informed in writing of the opening of the material.
- (3) Classified material to be carried by a courier shall be inventoried, a copy of the inventory shall be retained at the courier's office or duty location, and the courier shall carry a copy.

(4) Upon return, the courier shall return all classified material in a sealed package or, for any classified material that is not returned, produce a receipt signed by the security officer of the addressee organization.

(5) For guidance on hand-carrying NATO classified material, see Reference (ac).

e. Disclosure Authorization. In the event that the hand-carry of classified information shall also involve the disclosure of such information to foreign nationals, the DoD Component official responsible for approving the hand-carry is also responsible for ensuring a disclosure authorization is obtained in accordance with Reference (z).

13. ESCORT, COURIER, OR HAND-CARRY AUTHORIZATION. Responsible officials, as determined by DoD Component procedures, shall provide a written statement to each individual who is authorized to escort, courier, or hand-carry classified material. Procedures for authorizing on-site contractors to escort, courier, or hand-carry classified material shall comply with the requirements of References (x) and (ba). Authorization to escort, courier, or hand-carry SCI shall be in accordance with Reference (i).

a. The authorization statement may be contained in a letter, a courier card, or other written document, including travel orders. For travel aboard commercial aircraft, section 14 of this enclosure also applies. For international travel, also see the Appendix to this enclosure.

b. DoD (DD) Form 2501, "Courier Authorization," may be used to identify appropriately cleared DoD military and civilian personnel who have been approved to hand-carry classified material according to the following:

(1) The individual has a recurrent need to hand-carry classified information.

(2) An appropriate official in the individual's servicing security office signs the form.

(3) The form is issued for no more than 2 years at a time. The requirement for authorization to hand-carry classified information shall be reevaluated and/or revalidated at least once every 2 years, and a new form issued, if appropriate.

(4) Only the last four (4) digits of the individual's social security number shall be used in completing the DD Form 2501. Currently valid DD Forms 2501 shall be updated when renewed.

(5) The use of the DD Form 2501 for verification of authorization to hand-carry SCI or SAP information shall be according to policies and procedures established by the official having security responsibility for such information or programs.

14. HAND-CARRYING OR ESCORTING CLASSIFIED INFORMATION ON COMMERCIAL AIRCRAFT. Although pre-coordination is not typically required, in unusual

situations advance coordination with the local Transportation Security Administration (TSA) field office may be warranted to facilitate clearance through airline screening processes.

a. The individual designated as courier shall possess a DoD or contractor-issued identification card and a government-issued photo identification card. (If at least one of the identification cards does not contain date of birth, height, weight, and signature, include these items in the written authorization.)

b. The courier shall have a courier card or authorization letter prepared on letterhead stationary of the agency authorizing the carrying of classified material, which shall:

(1) Give the full name of the individual and his or her employing agency or company.

(2) Carry a date of issue and an expiration date.

(3) Carry the name, title, signature, and phone number of the official issuing the letter.

(4) Carry the name of the person and official U.S. Government telephone number of the person designated to confirm the courier authorization.

c. Upon arrival at the screening checkpoint the individual designated as courier shall ask to speak to the TSA Supervisory Transportation Security Officer and shall present the required identification and authorization documents. If the courier does not present all required documents, including valid courier authorization, DoD or contractor-issued identification card, and government-issued photo identification card, TSA officials will require the classified material to be screened in accordance with their standard procedures.

d. The courier shall go through the same airline ticketing and boarding process as other passengers. When the TSA Supervisory Transportation Security Officer confirms the courier's authorization to carry classified material, only the U.S. Government classified material is exempted from any form of inspection; the courier and all of the courier's personal property shall be provided for screening. The classified material shall remain within the courier's sight at all times during the screening process. When requested, the package(s) or the carry-on luggage containing the classified information may be presented for security screening so long as the courier maintains visual sight and the packaging or luggage is not opened.

e. Hand-carrying items aboard international commercial aircraft shall be done only on an exception basis. DoD travelers requiring access to classified materials at an overseas location shall exhaust all other transmission options (e.g., electronic file transfer, advance shipment by courier) before hand-carrying items aboard international commercial aircraft. See also sections 12 and 13, paying particular attention to paragraph 12.d. In addition to the requirements in the subparagraphs above, for international travel the authorization letter shall describe the material being carried (e.g., "three sealed packages (9" x 8" x 24")," addressee and sender) and the official who signed the authorization letter shall sign each package or carton to be exempt to facilitate its identification.

Appendix
Transfer of Classified Information or Material to Foreign Governments

APPENDIX TO ENCLOSURE 4

TRANSFER OF CLASSIFIED INFORMATION OR MATERIAL TO FOREIGN GOVERNMENTS

1. GENERAL

a. Transfers of classified information and material to a foreign government or international organization (hereinafter, "foreign government") may occur in the United States, in the recipient country, or in a third country. The risks of loss or compromise increase when classified information and material are transferred across international borders. Therefore, transfer arrangements must be thorough and clearly written. They must be understood and agreed to by the sending and receiving government officials involved in the transfer.

b. Transfers shall occur between government officials through official government-to-government channels (e.g., U.S. Government military transportation, Military Postal Service registered mail, Defense Courier Service, the Defense Transportation System). However, in some cases, it may not be possible to transfer the information and material through official government-to-government channels; the use of other channels may be necessary. These other channels may involve transfers by hand carrying or secure communications between cleared contractors or the use of cleared freight forwarders and commercial carriers.

c. Classified information or material, approved for disclosure in accordance with Reference (z), to be transferred to a foreign government or its representative shall be transferred only to a person or organization designated by the recipient government to sign for and assume custody and responsibility on behalf of the government. This designation should be in a letter of offer and acceptance (LOA), in a program agreement or arrangement or its implementing procedures, in a contract, or in a visit authorization. The designation shall contain assurances that the person to receive the information or material will have a security clearance at the appropriate level, that the person shall assume full security responsibility for the material on behalf of the foreign government, and that the information will be protected in accordance with the governing agreement or arrangement.

d. If other than government-to-government channels are to be used to transfer classified information or material to a foreign government, written transfer arrangements shall be approved by the DSAs of the sending and receiving governments, unless authority is delegated by a DSA, in writing, to a DGR of the respective sending or receiving government. The written arrangements shall provide for a DoD DGR or other DoD official to exercise oversight and ensure secure transfer from the point of origin to the ultimate destination, or to another agreed location where the recipient government's representative assumes responsibility. The information or material transferred shall be classified no higher than Secret.

e. Each LOA, agreement, contract, or other arrangement involving the disclosure or release of classified information or material to foreign governments shall either contain detailed transfer instructions or require that the DoD Component sponsoring the transaction and the recipient

government prepare and approve a separate plan for transferring the information or material. See section 10 of this appendix for required transportation plan content. If classified information or material is to be transferred from a non-governmental entity to a foreign government, it is also subject to the requirement of Reference (y).

f. U.S. Government communications and IT systems used for the transfer of classified information to foreign governments shall comply with paragraph 8.a. of Enclosure 4 of this Volume.

g. The requirements of this appendix do not pertain to:

(1) The disclosure or release of intelligence information and products under the purview of the DNI. Such disclosure or release shall be governed by policy issued by the DNI.

(2) Transfers of classified information and material during visits, which shall comply with Reference (q) and paragraph C3.2.7.6 of the Department of Defense Foreign Clearance Manual (Reference (be)).

2. RECEIPTS. Receipts are required for all transfers of classified information and material to a foreign government, except as noted in paragraphs 2.a. and 2.b. of this section. The receipts serve two important purposes. First, they document the transfer of security jurisdiction between the governments. Second, they alert the recipient government that the information or material has been transferred, and that it is responsible for protecting the information or material in compliance with the pertinent security or program agreement or arrangement.

a. Most foreign governments waive the receipt requirement for their restricted information.

b. Transmissions of classified information to a foreign government by IT and communications systems meeting the requirements of paragraph 1.f. of this appendix shall, at a minimum, be audited to assure that the intended recipient receives the information. The audit procedures for verifying receipt shall be commensurate with those specified in DoDI 8500.2 (Reference (bf)).

3. TRANSFERS BY DOD COMPONENT COURIER SERVICE, HAND-CARRYING, OR POSTAL SERVICE. Classified material that is of such size, weight, and configuration that it is suitable for transfer by an official DoD Component courier service, by a DoD employee approved to hand-carry classified information or material, or by U.S. Postal Service or Military Postal Service registered mail, shall be transferred in compliance with Enclosure 4 of this volume, and shall be delivered or addressed to:

a. An embassy, consulate, or other official agency of the recipient government having extraterritorial status in the United States; or

b. A U.S. Embassy or a U.S. military organization in the recipient country or in a third-party

country for delivery to a DGR or other designated representative of the recipient government.

4. TRANSFERS OF CLASSIFIED INFORMATION OR MATERIAL AS FREIGHT

a. Foreign Military Sales (FMS). DoD officials authorized to approve an FMS transaction involving the delivery of U.S. classified material to a foreign government shall, prior to any commitment on transfer arrangements, consult with supporting transportation officials to determine if secure U.S. Government transportation is available through U.S. Transportation Command or other DoD transportation authorities (e.g., Surface Deployment and Distribution Command, Military Sealift Command, Air Mobility Command) from the CONUS point of origin to the ultimate foreign destination, and to facilitate other modes of transfer when U.S. Government transportation is not available. Normally, the United States shall use the Defense Transportation System to deliver classified material resulting from FMS to the recipient government. The DoD Component FMS implementing agency that prepares the LOA shall develop a transportation plan in coordination with the foreign government. A generic transportation plan, containing standard security requirements necessary for any transfer, should be prepared during LOA negotiation. The LOA should specify responsibilities for completing the plan prior to the transfer of material. Security and transportation officials supporting the implementing agency shall evaluate and approve the transportation plan, in accordance with requirements of DoD 5105.38-M (Reference (bg)). If the plan is not satisfactory, the implementing agency will require that transfers be delayed until the plan is satisfactory.

b. Direct Commercial Sales. In accordance with Reference (x), transfers of classified material resulting from direct commercial sales shall comply with the same security standards that apply to FMS transfers, including the preparation of a generic transportation plan during contract negotiations.

c. Cooperative Programs. Transfer of classified information or material in support of a cooperative program shall be through official government-to-government channels or through other channels as agreed to by the respective governments (government-to-government transfer).

5. DELIVERY WITHIN THE UNITED STATES. Delivery of classified information or material to a foreign government at a point within the United States, using carriers specified in Enclosure 4 for the level of classified information or material involved, shall take place at:

a. An embassy, consulate, or other official agency under the control of the recipient government. An official designated by the foreign government as its DGR shall sign for the consignment.

b. The point of origin. When a DGR or other representative designated by the recipient government accepts delivery of classified material at the point of origin (e.g., a manufacturing facility or depot), the DoD DGR or other designated DoD official who transfers custody shall ensure that the recipient has a copy of the transportation plan and understands the secure means of onward movement of the classified material to its final destination, consistent with the

approved transportation plan. A freight forwarder or other transportation agent shall not be designated as a DGR. Such entities merely facilitate the shipment of the material and are subject to U.S. jurisdiction.

c. A military or commercial port of embarkation (POE) that is a recognized point of departure from the United States for on-loading aboard a ship, aircraft, or other carrier which is owned, controlled by, or registered to the recipient government. In such case, the transportation plan shall provide for U.S.-controlled shipment to the U.S. transshipment point and the identification of a cleared storage facility, U.S. Government or commercial, at or near the POE. The transportation plan shall identify the person who is to assume security oversight and control of the material while it is aboard the carrier. A DoD DGR or other designated U.S. Government official authorized to transfer custody shall supervise or observe the on loading of the classified material being transferred unless physical custody and security responsibility for the material is assumed by the recipient government's DGR prior to loading. In the event that transfer of physical and security custody cannot be accomplished promptly, the DoD official shall ensure that the classified material is either returned to a secure storage facility of the U.S. shipper, segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE, or held in a secure storage facility designated in the transportation plan.

d. A cleared freight forwarder facility identified by the recipient government in the transportation plan as its transfer agent. Unless the recipient government DGR is present to accept delivery of the classified material and receipt for it, to include acceptance of security responsibility on behalf of the recipient government, the DoD DGR shall maintain oversight until the recipient government DGR signs for and accepts such responsibility. The freight forwarder is a transfer agent and shall not be the recipient government's DGR.

6. DELIVERY OUTSIDE THE UNITED STATES

a. Within the Recipient Country. Classified material to be delivered to a foreign government within the recipient country shall be delivered on arrival in the recipient country to a U.S. Government representative who shall arrange for its transfer to a DGR or other recipient government representative identified in the transportation plan. If a U.S. Government official authorized to accomplish the transfer of custody escorts the shipment, the material may be delivered directly to the recipient government's DGR or other recipient government representative upon arrival.

b. In a Third Country. Classified material to be delivered to a foreign government representative within a third country shall be delivered to an agency or installation of the United States, or of the recipient government, that has extraterritorial status or otherwise is exempt from the jurisdiction of the third country. Unless a U.S. Government official authorized to accomplish the transfer of custody escorts the material, a U.S. Government official shall be designated locally to receive the shipment upon arrival and deliver it to a DGR or other recipient government representative identified in the transportation plan.

7. USE OF INTERNATIONAL CARRIERS. Transfers of classified material to locations outside the United States shall be made only via ships, aircraft, or other carriers as specified in Enclosure 4 of this Volume.

8. ESCORTS. Escorts are required aboard the carrier when transfers to a foreign government are to occur outside the United States. Escorts shall possess personnel security clearances of at least the same classification level as the material to be transferred. The escorts shall be provided by the implementing agency for FMS cases or by the U.S. cleared contractor for direct commercial sales, unless:

a. The material is shipped by U.S. military carrier and the crew assumes control of the material.

b. The recipient government DGR has signed for the consignment, a recipient-government military carrier or carrier owned by or registered to the recipient government is used, and the recipient government provides the cleared escort.

c. The exception authorized in paragraph 4.j. of Enclosure 4 is used and the conditions of that paragraph are met.

9. RETURN FOR REPAIR, MODIFICATION, OR MAINTENANCE. Foreign governments may return classified material for repair, modification, or maintenance. The requirements for return shipment shall be specified in the LOA for FMS and in the security requirements section of a direct commercial sales contract. The transfer procedures shall be in the original transportation plan and shall include the same details on transportation channels, routes, transfer points, and identity of responsible officials as specified for the original transfer.

10. TRANSPORTATION PLAN. The transportation plan required by paragraph 1.e. of this appendix shall, at a minimum, include:

a. The purpose of the plan (i.e., FMS or direct commercial sale, with FMS case designator or commercial contract identification), purchasing government, and date.

b. A description of the material to be shipped, identification of the associated FMS case or contract line item(s), munitions list category, and classification.

c. A description of packaging requirements, seals, and storage requirements during shipment.

d. Identification, by name, title, organization of the DGRs, security and transportation officials who will arrange the transfer of, sign receipts for, and assume security responsibility for the freight during the transfer process. Mailing addresses, telephone numbers, fax numbers, and e-mail addresses must be listed for each government's representatives.

e. Identification and specific location(s) of the delivery points, transfer points, and/or processing points and description of the security arrangements for the material while located at each point; if transfers will occur between carriers, explain the process, including the identification of persons who will be involved.

f. Identification of commercial entities that will be involved in the shipping process (e.g., carriers and freight forwarders or transportation agents), the extent of their involvement, and their clearance. Include names, addresses, telephone and fax numbers, e-mail addresses, and points of contact.

g. A description of each segment of the route to be taken and, if applicable, security arrangements for overnight stops or delays.

h. Arrangements for dealing with port and carrier security, immigration, and customs officials. Identify personnel from each who have been consulted (and an alternate), and their telephone and fax numbers, and e-mail addresses.

i. Names of escorts (and who they represent) or other responsible officials (e.g., Captain or crew chief) to be used, including their government identification, passport numbers, security clearances, and details concerning their responsibilities. Describe procedures for their accessibility to the material while in storage. If the shipment will occur on a recurring basis, the shipper shall provide an updated list of escorts with their identifying data prior to each shipment in accordance with provisions of the approved plan.

j. A description of emergency procedures, and who is responsible for actions that must be taken in the event of an emergency (e.g., unexpected stop anywhere along the route). Identify individuals by name, and provide their organization, telephone and fax numbers, and e-mail addresses.

k. Procedures for loading and securing the material.

l. Procedures for unloading the material and dealing with government port security, customs, and immigration officials.

m. Identification, by name and personal identification, of the person who will ultimately sign for and assume final control of the material for the recipient government.

n. A requirement for the recipient government to examine shipping documents upon receiving classified material in its own territory and notify the DoD Component responsible for security of the classified material if the material has been transferred en route to any carrier not authorized by the transportation plan.

o. A requirement for the recipient government to inform the DoD Component responsible for the security of the classified material promptly and fully of any known or suspected compromise of the classified material.

p. Specific, detailed arrangements for return shipments for repair, overhaul, modification, or maintenance (see section 9 of this appendix).

ENCLOSURE 5

SECURITY EDUCATION AND TRAINING

1. REQUIREMENT. The Heads of the DoD Components shall ensure that their personnel receive security education and training that:

- a. Provides necessary knowledge and information to enable quality performance of security functions.
- b. Promotes understanding of DoD Information Security Program policies and requirements and their importance to national security and national interests.
- c. Instills and maintains continuing awareness of security requirements.
- d. Assists in promoting a high degree of motivation to support program goals.

2. SECURITY EDUCATION AND TRAINING RESOURCES

a. Security education and training may be accomplished by establishing programs within the DoD Component, using external resources such as the Defense Security Service Academy, or a combination of the two.

b. DoD Components may, if desired, combine into one overall program the education and training requirements of this enclosure and those for CUI specified in Volume 4 of this Manual.

3. INITIAL ORIENTATION. All personnel in the organization, including DoD civilians, military members, and on-site support contractors shall receive an initial orientation to the DoD Information Security Program.

a. This initial orientation is intended to:

(1) Define classified information and CUI and explain the importance of protecting such information.

(2) Produce a basic understanding of security policies and principles.

(3) Notify personnel of their responsibilities within the security program, and inform them of the administrative, civil, and/or criminal sanctions that can be applied when appropriate.

(4) Provide individuals enough information to ensure the proper protection of classified information and CUI in their possession, including actions to be taken if such information is discovered unsecured, a security vulnerability is noted, or a person has been seeking

unauthorized access to such information.

(5) Inform personnel of the need for review of ALL unclassified DoD information prior to its release to the public.

b. Security educators shall also consider including in the initial orientation identification of the DoD Component senior agency official and activity security management personnel, a description of their responsibilities, and whether they are involved in the protection of classified or controlled unclassified information. If not included in the initial orientation, such information must be included in the training required by paragraph 3.c. of this section.

c. In addition to the requirements in paragraphs 3.a. and 3.b. of this section, upon initial access to classified information, all personnel shall receive training on security policies and principles and derivative classification practices, including:

(1) The definition of classified information, the levels of classified information, and the damage criteria associated with each level.

(2) The responsibilities of DoD personnel who create or handle classified information, including:

(a) The requirements for controlling access to classified information, including:

1. The general conditions for and restrictions on access to classified information.

2. The steps an individual shall take when he or she is asked to verify classified information disclosed through unofficial open sources (e.g., news media, periodicals, and public websites).

(b) The policies and procedures for safeguarding classified information, including:

1. The proper methods and procedures for using, storing, reproducing, transmitting, disseminating, and destroying classified information.

2. The steps an individual shall take to safeguard classified information during an emergency evacuation situation.

3. The steps an individual shall take when he or she believes classified information has not been, or is not being, properly protected.

(c) The accountability of derivative classifiers for the accuracy of their work.

(3) An explanation that derivative classification is extracting, paraphrasing, or restating classified information based on a security classification guide, one or more source documents, or both.

(4) The authorized types of sources that can be used for derivative classification and where to obtain them, including:

(a) An explanation that a security classification guide:

1. Is precise, comprehensive guidance regarding specific program, system, operation or weapon system elements of information to be classified, including classification levels, reasons for classification, and the duration of classification.

2. Is approved and signed by the cognizant OCA.

3. Is an authoritative source for derivative classification.

4. Ensures consistent application of classification to the same information.

(b) How to use a security classification guide or other derivative source.

(c) How and where to obtain classification guidance currently available for a specific area of expertise, including:

1. The security manager and/or the program or project office.

2. The Defense Technical Information Center, at www.dtic.mil (registration required).

3. In the case of a military operation and the creation or execution of plans and orders thereto, the higher headquarters office that mandated or directed the operation or mission.

(5) The proper and complete classification markings to be used for classified information, and how those markings are to be applied, including:

(a) The importance of properly applying the authorized classification markings and the need to avoid over-classification.

(b) How to document the level of classification, duration of classification and the source(s) of classified information included in the material (e.g., document, e-mail, briefing, video) being created or generated.

(c) How to observe and respect the original classification decision(s).

(d) How to maintain lists of sources when multiple sources of classification are used.

(e) How to determine the duration of classification.

(f) How to properly use control markings to limit or expand distribution, including foreign disclosure and release markings (e.g., "REL TO" (releasable to), "NOFORN" (not

releasable to foreign nationals) and DISPLAY ONLY).

(g) How to challenge classification decisions.

(h) How to downgrade or declassify information as an authorized holder of information in accordance with the direction of the cognizant OCA or classification guide.

(i) How to mark and share “working papers” and other drafts, including the requirements for such markings.

(6) The definition of a security incident, a violation and a compromise of classified information, examples of each, and an explanation of the criminal, civil, and administrative sanctions that may be taken against an individual who fails to comply with program requirements or to protect classified information from unauthorized disclosure.

(7) The policies and procedures for sharing classified information with state, local, tribal, and private sector officials and with foreign governments and international organizations, including the markings that designate information as qualifying for sharing, if appropriate for the activity’s mission or function.

(8) The policies and procedures for the marking, safeguarding, and accounting of NATO classified information.

d. In addition to the training specified by paragraphs 3.a through 3.c of this section and information assurance (IA) training required by DoDD 8570.01 (Reference (bh)), personnel who are authorized access to classified information systems shall receive training which specifically addresses:

(1) Proper use of information systems for creating, using, storing, processing, or transmitting classified information.

(2) The requirement for and application of markings, including portion markings, to information in electronic formats (e.g., documents, e-mail, briefings, web-based information, databases, spreadsheets).

(3) Marking, handling, storage, transportation, and destruction of classified computer media (e.g., floppy disks, CDs, DVDs, removable hard drives).

(4) Procedures to be followed when using classified removable data storage media.

(5) Procedures to be followed if an individual believes an unauthorized disclosure of classified data has occurred on an information system or network (typically called a “data spill”).

4. SPECIAL TRAINING REQUIREMENTS

a. Individuals with specified duties in the Information Security Program, as identified in sections 5, 6, and 10 of this enclosure, shall be provided security education and training commensurate with job responsibilities and sufficient to permit effective performance of those duties. The education and training may be provided before, concurrent with, or not later than 6 months following assuming those duties, unless otherwise specified.

b. Deployable organizations shall provide, prior to deployment, enhanced security training to meet the needs of the operational environment. Where appropriate, this pre-deployment training shall specifically address security requirements associated with information sharing (e.g., release of information to state, local, tribal, or coalition partners; use and handling of FGI) and shall provide training on the classification markings that are to be applied in these situations and that designate information as qualifying for sharing.

c. Additional security education and training may be required for personnel who:

(1) Travel to foreign countries where special concerns about possible exploitation exist or attend professional meetings or conferences where foreign attendance is likely.

(2) Escort, hand-carry, or serve as a courier for classified material.

(3) Are authorized access to classified information requiring special control or safeguarding measures.

(4) Are involved with international programs.

(5) Are involved with acquisition programs subject to Reference (af).

(6) Are involved with FGI, or work in coalition or bilateral environments, or in offices, activities, or organizations hosting foreign exchange officers.

(7) Submit information to OCAs for original classification decisions and therefore need additional knowledge of the original classification decision process.

5. OCA TRAINING. Training for newly appointed OCAs shall be provided prior to exercise of the authority and each OCA shall receive training annually thereafter as required in paragraph 7.b. of this enclosure. The OCA shall certify in writing that the training has been received. Personnel preparing recommendations for original classification to OCAs will receive the same training. The training shall address OCA responsibilities and classification principles, proper safeguarding of classified information, and the criminal, civil, and administrative sanctions that may be brought against an individual. At a minimum, the training shall address:

a. General requirements, including:

(1) The difference between original and derivative classification.

(2) Persons who can classify information originally.

(a) OCA is assigned to a position, not a person and, except as authorized by Enclosure 4 of Volume 1 of this Manual, may not be further delegated.

(b) Only individuals carrying out a unique mission with responsibility in one of the subject areas prescribed by section 1.4 of Reference (d) may be designated an OCA.

(c) Deputies, vice commanders, chiefs of staff, and similar immediate subordinates of an OCA are empowered to exercise OCA when they have been officially designated to assume the duty position of the OCA in an acting capacity during the OCA's absence and have certified in writing that they have received required OCA training.

(3) The requirement to certify, in writing, before initially exercising OCA authority and annually thereafter, that training has been received.

(4) The prohibitions and limitations on classifying information, as stated in sections 1 and 2 of Enclosure 4 of Volume 1 of this Manual, and the need to avoid over classification.

b. The responsibility and discretion the OCA has in classifying information.

(1) OCAs must be aware that their decisions to classify information have a substantial impact on the operations of the Department and on national security. Others who work with the information use these original decisions to make proper derivative classification decisions and to assure that the information is properly protected from unauthorized disclosure.

(2) OCAs are accountable to the Secretary of Defense for their classification decisions.

(3) OCAs shall exercise a substantial degree of autonomy in operations or mission. Information warranting original classification must be developed in the normal course of actions or activity.

c. The classification principles and process specified in section 6, Enclosure 4 of Volume 1 of this Manual.

(1) Original classification requires identification of specific elements of information which could adversely affect the national security if compromised. In addition to consideration of harm to the national security, OCAs must weigh the advantages and disadvantages of classifying each element and should consider, when applicable:

(a) Degree of intended or anticipated dissemination or use.

(b) Net national advantage.

(c) Lead time advantage for operational or technological use.

- (d) Cost in terms of time, money, and personnel.
- (e) Impact on attaining the program objective.
- (f) State of the art and public knowledge of the U.S. interest.
- (g) Appearance in the public domain, inadvertent disclosure or other compromise.
- (h) Basic scientific research data or unusually significant scientific findings.
- (i) Association or compilation of information or data.

(2) Information is classified either because its unauthorized disclosure could reasonably be expected to cause identifiable or discernable damage to national security or because it may reveal such information when associated with other information. If information is classified in compilation with other information, a clear explanation of rationale must be provided (see section 12 of Enclosure 3 of Volume 2).

(3) OCAs shall ensure that a review for possible declassification is conducted expeditiously in the event of compromise, that damage assessments are conducted as necessary, and that formal challenges to classification, classification conflicts, and requests for classification determinations from individuals who are not OCAs are addressed as required by this Manual.

d. The procedures that must be followed when making and communicating original classification decisions.

(1) The required markings that must appear on classified information as specified in Volume 2, Enclosure 3 of this Manual.

(2) The process for determining duration of classification.

(a) Information shall be assigned a date or event for declassification that is 25 years or less from the date of origination, except for information that is clearly and demonstrably expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction.

(b) Information in records with permanent historic value may be classified for longer than 25 years only if the Interagency Security Classification Appeals Panel (ISCAP) has been notified of such a date in accordance with the procedures in section 13, Enclosure 5 of Volume 1 of this Manual. The ISCAP decisions will be codified in a classification or declassification guide.

(3) The general standards and procedures for changes in classification (downgrade, upgrade, declassify) and the general requirements for automatic and systematic declassification and mandatory reviews for declassification.

(a) An OCA should organize the classification process around time and event-phased downgrading and declassification events to the maximum extent possible.

(b) An OCA may change the level of classification of information under their jurisdiction (downgrade, upgrade, declassify) as specified in section 7, Enclosure 4 of Volume 1 of this Manual.

(c) Classification may change at each phase of an operation, research and development cycle, or acquisition, as determined by the OCA with responsibility over the information.

(4) The requirements and standards for creating, issuing, and maintaining security classification guidance, including classification and declassification guides, as identified in section 8, Enclosure 4 of Volume 1 of this Manual.

e. The proper safeguarding protections to apply when using, storing, reproducing, transmitting, disseminating, and destroying classified information.

f. The criminal, civil, and administrative sanctions that may be brought against an individual who fails to classify information properly or to protect classified information from unauthorized disclosure.

6. DECLASSIFICATION AUTHORITY TRAINING. The security education and training provided declassification authorities other than original classifiers shall, at a minimum, address:

a. The standards, methods, and procedures for declassifying information pursuant to References (d) and (f) and this Manual.

b. The standards for creating, maintaining, and using declassification guides.

c. The information contained in the DoD Component's declassification plan.

d. The DoD Component's responsibilities for establishing and maintaining a declassification database.

e. The referral process and requirements.

7. ANNUAL REFRESHER TRAINING

a. At a minimum, all DoD civilians, military members, and on-site support contractors with access to classified information shall receive annual refresher training that reinforces the policies, principle, and procedures covered in their initial and specialized training. Refresher training shall also address the threat and the techniques foreign intelligence activities use while

attempting to obtain classified DoD information, and advise personnel of penalties for engaging in espionage activities and other unauthorized disclosures. Refresher training shall also address relevant changes in information security policy or procedures and issues or concerns identified during DoD Component self-inspections. Information system users shall additionally complete an annual IA awareness refresher, as required by Reference (bh).

b. Each OCA shall receive annual training as specified in section 5 of this enclosure. The OCA shall certify receipt of the training in writing. OCAs who do not receive the specified training at least once within a calendar year shall have their classification authority suspended by the DoD Component Head or the senior agency official who delegated the authority until the training has taken place, unless a waiver is granted in accordance with paragraph 7.f of this section.

c. Derivative classifiers (i.e., those who create new documents, including e-mails, based on existing classification guidance) shall receive training in derivative classification as required by paragraph 3.c. of this enclosure, with an emphasis on avoiding over-classification, at least once every 2 years. Training may, at the DoD Component's discretion, be included in the training required by paragraph 7.a. of this section. Derivative classifiers who do not receive training at least once every 2 years shall not be authorized or allowed to derivatively classify information until they have received training, unless a waiver is granted in accordance with paragraph 7.f of this section.

d. Declassification authorities shall receive training as required by section 6 of this enclosure at least once every 2 years.

e. DoD Components shall track training required by paragraphs 7.b and 7.c of this section and take appropriate action to suspend OCA authority in accordance with paragraph 7.b or disallow derivative classification in accordance with paragraph 7.c if the training is not accomplished as required.

f. A waiver to the training requirement in paragraphs 7.b or 7.c of this section may be granted by the DoD Component Head, the Deputy Component Head, or senior agency official if an individual is unable to receive required training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive the required training as soon as practicable.

8. CONTINUING SECURITY EDUCATION AND TRAINING. Security education and training shall be continuous, rather than aperiodic. Periodic briefings, training sessions, and other formal presentations shall be supplemented with other information and promotional efforts to ensure that continuous awareness and performance quality is maintained. The use of job performance aids and other substitutes for formal training is encouraged when they are determined to be the most effective means of achieving program goals. The circulation of directives or similar material on a read-and-initial basis shall not be considered as the sole means of fulfilling any of the specific requirements of this enclosure.

9. TERMINATION BRIEFINGS. The DoD Components shall establish procedures to ensure that cleared employees who leave the organization or whose clearance is terminated receive a termination briefing in accordance with paragraph C9.2.5 of Reference (l). The briefing shall:

- a. Emphasize their continued responsibility to protect classified and controlled unclassified information to which they have had access.
- b. Provide instructions for reporting any unauthorized attempt to gain access to such information.
- c. Advise the individuals of the prohibitions against retaining classified and controlled unclassified material when leaving the organization.
- d. Identify the requirement that retired personnel, former DoD employees, and non-active duty members of the Reserve Components must submit writings and other materials intended for public release to the DoD security review process as specified by Reference (k).
- e. Remind them of the potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

10. MANAGEMENT AND OVERSIGHT TRAINING. Individuals designated as security managers, classification management officers, security specialists, or any other personnel whose duties significantly involve managing and overseeing classified information shall receive training that meets the requirements of DoDI 3305.13 (Reference (bi)) and addresses:

- a. The original and derivative classification processes and the standards applicable to each.
- b. The proper and complete classification markings to be applied to classified information,
- c. The proper use of control markings to limit or expand distribution, including foreign disclosure and release markings (e.g., REL TO, NOFORN, and DISPLAY ONLY).
- d. The authorities, methods, and processes for downgrading and declassifying information.
- e. The methods for properly using, storing, reproducing, transmitting, disseminating, and destroying classified information.
- f. The requirements for creating, maintaining, and issuing classification and declassification guides.
- g. The requirements for controlling access to classified information.
- h. The procedures for investigating and reporting instances of actual or potential compromise of classified information, including when in electronic form, and the penalties that may be associated with violating established security policies and procedures.

i. The requirements for creating, maintaining, and terminating SAPs, and the mechanisms for monitoring such programs.

j. The procedures for the secure use of information systems and networks that use, process, store, reproduce, or transmit classified information, and requirements for their certification and accreditation.

k. The provisions for automatic declassification and the need for systematic and mandatory reviews for declassification, and the DoD Component procedures for accomplishing each.

l. The requirements for overseeing the Information Security Program, including self-inspections.

11. PROGRAM OVERSIGHT. The Heads of the DoD Components shall ensure that security education and training are appropriately evaluated during self-inspections and other oversight activities. This evaluation shall include assessing the quality and effectiveness of the efforts, as well as ensuring appropriate coverage of the target populations. The Heads of the DoD Components shall require maintaining records of education and training offered and employee participation, as they deem necessary to permit effective oversight.

ENCLOSURE 6

SECURITY INCIDENTS INVOLVING CLASSIFIED INFORMATION

1. INTRODUCTION. Protection of classified information is essential to maintaining security and achieving mission success in DoD operational and warfighting environments. Prompt reporting of security incidents ensure that such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of an actual loss or unauthorized disclosure of classified information and to preclude recurrence through an informed, properly tailored, and up-to-date security education and awareness program. In cases where compromise has been ruled out and there is no adverse effect on national security, a common sense approach to the early resolution of an incident at the lowest appropriate level is encouraged. All security incidents involving classified information shall involve a security inquiry, a security investigation, or both.

a. The terms associated with security incidents are formally defined in the Glossary, but to ensure common understanding, the following general characterizations are provided:

(1) Infraction. An infraction is a security incident involving failure to comply with requirements (i.e., the provisions of References (d) and (f), this Manual or other applicable security policy) which cannot reasonably be expected to, and does not, result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent. While it does not constitute a security violation, if left uncorrected, can lead to security violations or compromises. It requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

(2) Violation. Violations are security incidents that indicate knowing, willful, and negligent for security regulations, and result in, or could be expected to result in, the loss or compromise of classified information. Security violations require an inquiry and/or investigation.

(a) Compromise. A compromise is a security incident (more specifically, a violation) in which there is an unauthorized disclosure of classified information (i.e., disclosure to a person(s) who does not have a valid clearance, authorized access, or a need to know).

(b) Loss. A loss occurs when classified information cannot be physically located or accounted for (e.g., classified information/equipment is discovered missing during an audit and cannot be immediately located).

(3) Inquiry. An inquiry is fact-finding and analysis conducted to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information. The inquiry identifies the facts, characterizes the incident as an infraction or a violation, identifies if possible the cause(s) and person(s) responsible, reports corrective actions taken or to be taken, and makes recommendations as to the need for further corrective action or a more in-depth investigation. Inquires, generally, are

initiated and conducted at the lowest echelon possible within the DoD Component.

(4) Investigation. An investigation is conducted for a security violation when the incident cannot be resolved via inquiry or for incidents where an in-depth and comprehensive examination of the matter is appropriate.

b. Certain practices dangerous to security, while not reportable as security incidents, have the potential to jeopardize the security of classified information and material if allowed to perpetuate. Examples of such practices are: placing a paper recycling box next to a classified copier or placing burn bags next to unclassified trash containers; stopping at a public establishment to conduct personal business while hand-carrying classified information; or failing to change security container combinations promptly when required. These practices, when identified, must be promptly addressed by security management and appropriate changes made, actions taken, or training provided, to ensure the security of classified information.

2. CONSEQUENCES OF COMPROMISE. The compromise of classified information presents a threat to the national security and may damage intelligence or operational capabilities; lessen the DoD ability to protect critical information, technologies, and programs; or reduce the effectiveness of DoD management. Once a compromise is known to have occurred, the seriousness of damage to U.S. national security or the extent of the adverse affect on the national security must be determined and appropriate measures taken to negate or minimize the adverse effects. When possible, action shall also be taken to regain custody of documents or material that was compromised. In all cases, security management must take appropriate action to identify the source and reason for the suspected or actual compromise and take remedial action to prevent recurrence.

3. REPORTING AND NOTIFICATIONS

a. Anyone finding classified information out of proper control shall, if possible, take custody of and safeguard the material and immediately notify the appropriate security authorities. Secure communications should be used for notification whenever possible.

b. Every civilian employee and Active, Reserve, and National Guard Military member of the Department of Defense, and every DoD contractor or employee of a contractor working with classified material, as provided by the terms of the contract, who becomes aware of the loss or potential compromise of classified information shall immediately report it to the head of his or her local activity and to the activity security manager.

c. If the person believes that the head of the activity or the security manager may have been involved in or responsible for the incident, he or she may report it to the security authorities at the next higher level of command or supervision. If circumstances of discovery make such notification impractical, the individual shall notify the commanding officer or security manager at the most readily available DoD facility or contact any DoD law enforcement, counterintelligence (CI), or Defense criminal investigative organization (DCIO).

d. Activity security officials shall advise their chain of command of compromises occurring within their area of security responsibility or involving assigned personnel.

e. If the head of an activity or the activity security manager to whom an incident is initially reported does not have security cognizance over the incident, such official shall ensure that the incident is reported to the appropriate authority. The organization with security cognizance shall ensure that an inquiry and, when appropriate, investigation are conducted, as needed, consistent with the requirements of this enclosure and corrective action is taken as required.

f. Reporting confirmed security incidents to the Director of Security, OUSD(I), is necessary when the incidents have or may have significant consequences or the fact of the incident may become public. Such incidents shall be reported promptly through appropriate security channels by the DoD Component senior agency official. When appropriate, preliminary reports shall be provided, particularly when the fact of the incident may become public or attract media attention.

(1) The Director of Security, OUSD(I), shall be notified of:

(a) A violation involving espionage.

(b) An unauthorized disclosure of classified information in the public media. See section 7 of this enclosure for information required in the notification. Additional notification is not required for reference to or republication of a previously identified media disclosure.

(c) Any violation wherein properly classified information is knowingly, willfully, or negligently disclosed to unauthorized persons or information is classified or continues to be classified when that violation:

1. Is reported to the oversight committees of Congress;

2. May attract significant public attention;

3. Involves large amounts of classified information; or

4. Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(d) Any violation wherein a SAP is knowingly, willfully, or negligently created or continued contrary to the requirements of Reference (ah), DoDI O-5205.11 (Reference (bj)), this Manual, and national policies.

(e) A security failure or compromise of classified information relating to any defense operation, system, or technology that is likely to cause significant harm or damage to U.S. national security interests, for which Congressional reporting may be required by section 2723 of title 10, U.S.C. (Reference (bk)).

(f) Other egregious security incident (as determined by the DoD Component senior agency official).

(2) Security incidents that do not meet the reporting criteria specified above shall be filed in a retrievable format by the DoD Component and shall be available for inspection or further analysis, review, and potential investigation.

(3) On behalf of the Secretary of Defense, the USD(I) shall notify Congress and the Director, ISOO, regarding specific cases or incidents as required by References (d) and (bk).

(4) The Director of Security, OUSD(I), shall coordinate with the Office of the DNI (ODNI) National Counterintelligence Executive (NCIX) as needed to ensure notifications required by Intelligence Community Directive 701 (Reference (bl)) are made.

4. CLASSIFICATION OF REPORTS

a. Security incident reports shall be classified according to the content of the report and at the level prescribed by the applicable program security classification guides. At a minimum, reports shall be designated FOUO and marked as required by Volume 4 of this Manual, in order to provide appropriate protection for information regarding personnel involved and information that could facilitate unauthorized access to classified information. If the lost or compromised information is beyond the jurisdiction of the U.S. Government and cannot be recovered (e.g., media leak, public website posting, or loss in a foreign country), the report and location of the compromise (e.g., geographic location of unrecoverable equipment) shall be classified commensurate with the classification level of the compromised material to prevent further unauthorized disclosure.

b. If an FOUO report is to be disseminated outside the Department of Defense (e.g., to another Federal agency), the face of the document shall bear an expanded marking, as specified in Enclosure 3 of Volume 4 of this Manual, stating that the information may be exempt from mandatory disclosure pursuant to section 552 of title 5, U.S.C. (also known as “The Freedom of Information Act” and hereinafter referred to as “FOIA” (Reference (bm))).

c. Reports, whether classified or unclassified, disclosing technical data shall be marked with the appropriate distribution statement as described in DoDD 5230.24 (Reference (bn)) or associated with the information involved in the incident.

5. SPECIAL CIRCUMSTANCES. Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements as specified in paragraphs 5.a through 5.o.

a. Security Incidents Involving Deliberate Compromise, a Foreign Intelligence Service or a Terrorist Organization. Any incident in which deliberate compromise of classified information or involvement of a foreign intelligence service, international terrorist group, or organization is

suspected shall be reported immediately to the cognizant Defense CI component, in accordance with DoDD 5240.06 (Reference (bo)). Security officials shall not initiate or continue an inquiry or investigation of the incident unless it is fully coordinated with the cognizant Defense CI component.

b. Security Incidents Involving Apparent Violations of Criminal Law. Any incident in which an apparent violation of criminal law is suspected, but which is reasonably not believed to be espionage or involving matters described in paragraph 5.a of this section, shall be reported immediately to the local DCIO. If that organization accepts jurisdiction and initiates action, coordinate with them prior to taking any further action on the security inquiry or investigation so as not to jeopardize the integrity of either investigation.

c. Security Incidents Involving COMSEC or Cryptologic Information. Actual or potential compromises involving cryptographic information shall be handled according to NSTISSI 4003 (Reference (bp)).

d. Security Incidents Involving SCI. Actual or potential compromises involving SCI shall be reported to the activity SSO and handled in accordance with References (i) and (bl).

(1) Incidents involving SCI that meet the criteria in paragraph 3.f of this enclosure shall also be reported to the Director of Security, OUSD(I).

(2) If a DoD Component believes a disclosure may contain classified SCI information under the control of an(other) Intelligence Community agency, the DoD Component shall notify NCIX. NCIX shall coordinate notification to the affected agency.

e. Security Incidents Involving RD and/or FRD. In accordance with the provisions of section 3161 of Public Law 105-261 (Reference (bq)), and its implementing plan, the Secretary of Energy must report to Congress inadvertent disclosure of RD or FRD occurring pursuant to automatic declassification processes. Components shall notify the Department of Energy as necessary and provide a copy of the notification to the Deputy Assistant Secretary of Defense for Nuclear Matters and the Director of Security, OUSD(I).

f. Security Incidents Involving IT. Actual or potential compromises of classified information involving IT, automated information systems, or computer systems, terminals, or equipment shall be reported, in accordance with Reference (bf), through appropriate channels by the IA manager (IAM) to the activity security manager. Inquiries into and resolution of incidents involving compromise of classified information resident on computers or in IT systems require coordination with and assistance from the local IA officials, but prompt resolution remains the responsibility of the activity security manager. See Enclosure 7 for additional guidance on handling of classified data spills.

g. Security Incidents Involving FGI or NATO Information. Actual or potential compromises involving FGI or NATO information shall also be reported promptly by the DoD Component senior agency official to the USD(P), who serves as the DSA. The Director, International Security Programs, Defense Technology Security Administration, OUSD(P), shall be

responsible, on behalf of the DSA, for notifying and coordinating with NATO or the foreign government, as appropriate.

h. Security Incidents Involving Classified U.S. Information Provided to Foreign Governments. Actual or potential compromises of U.S. classified information held by foreign governments shall be reported to the originating DoD Component, the OCA, the Director of Security, OUSD(I), and the Director, International Security Programs, Defense Technology Security Administration, OUSD(P).

i. Security Incidents Involving SAPs. Actual or potential compromises involving DoD SAPs, or results of inquiries and/or investigations that indicate that weaknesses or vulnerabilities in established SAP policy and/or procedures contributed to an actual or potential compromise, shall be reported by the DoD Component SAP program office to the DoD SAP Central Office, which shall report to the Director of Security, OUSD(I).

j. Security Incidents Involving Improper Transfer of Classified Information. Any activity that receives classified information that has been improperly handled, addressed, packaged, transmitted, or transported shall make a determination as to whether the information has been subjected to compromise. If the activity determines that the classified information has been subjected to compromise, the receiving activity shall immediately notify the sending activity, which shall be responsible for initiating an inquiry or investigation, as appropriate. The receiving activity shall share information generated regarding the incident with the sending activity. The sending activity is responsible for required notifications (e.g., to the OCA). Classified information shall be considered as having been subjected to compromise if it has been handled through foreign postal systems, its shipping container has been damaged to an extent that the contents are exposed, or it has been transmitted (e.g., telephone, facsimile, message, e-mail, computer or data links) over communications circuits that are not approved for transmission of classified information. If the receiving activity determines that classified information was not in fact compromised, but was nevertheless improperly prepared or transferred, the receiving activity shall report the discrepancy to the sending activity.

k. Security Incidents Involving On-Site Contractors. Security incidents, including any inquiries or investigations required, involving on-site contractors shall be handled in accordance with paragraph C1.1.9 of Reference (ba). As specified by paragraph C1.1.9 of Reference (ba) and paragraph 6-105c of Reference (x), host activity security rules and procedures apply. Disciplinary action and sanctions are the responsibility of the contractor's company unless specific contract provisions address such actions. Security managers shall furnish the results of inquiries to the company, with a copy to Defense Security Service, in order to facilitate such action. Specified U.S. Government officials retain the ability, when appropriate and in accordance with the authorities and requirements of Reference (ba), to deny access to classified information, to revoke or suspend security clearances, and to take certain other administrative actions, such as to deny an individual continued access to the facility.

l. Security Incidents Involving Critical Program Information (CPI). Upon learning that classified CPI or CPI related to classified contracts may have been or was actually compromised, security officials shall inform the program manager of record and the cognizant Defense CI

component pursuant to DoDD O-5240.02 (Reference (br)). The specific CPI involved in the incident should be identified in inquiry and investigation reports. Classify reports as required by the applicable program security classification guide(s).

m. Security Incidents Involving ACCM-Protected Information. Security officials shall refer to section 18 of Enclosure 2 of this Volume for additional guidance on security incidents involving ACCM-protected information as well as safeguarding and handling of ACCM-protected information.

n. Absence Without Authorization. When an individual who has had access to classified information is absent without authorization, the head of the activity or security manager shall determine if there are indications of activities, behavior, or associations that could indicate classified information may be at risk. If so, the supporting Defense CI component shall be notified in accordance with Reference (br). The scope and depth of the inquiry shall depend on the length of absence and the sensitivity of the classified information involved. Missing personnel authorized SCI access shall be reported in accordance with Reference (i).

o. Coordination with Legal Counsel and the Department of Justice (DoJ). Whenever formal action, beyond adjudication of a finding of a security violation and assignment of reprimand or disciplinary action at the activity level is contemplated against any person believed responsible for the unauthorized disclosure of classified information, DoD Component officials shall coordinate with servicing legal counsel. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, Component officials shall use established procedures and channels to ensure coordination with the legal counsel of the DoD Component or Federal agency where the individual is assigned or employed and the DoJ.

6. SECURITY INQUIRIES AND INVESTIGATIONS

a. Requirement. All known or suspected instances of unauthorized disclosure of classified information shall be promptly addressed by the cognizant DoD Component to decide the nature and circumstances of the disclosure and the extent of damage to national security, and appropriate corrective action shall be taken. See Appendix 1 to this enclosure for a sample, optional format for use in documenting actions. Reports of inquiries and investigations, at a minimum, shall be designated and marked as FOUO.

b. Coordination with Criminal Investigative Organization or Defense CI Component. When information suggestive of a criminal or CI nature is discovered, all actions associated with the inquiry or investigation shall cease pending coordination with the cognizant DCIO or Defense CI component. If the DCIO or Defense CI component accepts jurisdiction, the inquiry or investigation shall not be resumed without agreement of the cognizant criminal investigative organization or CI component. All relevant information shall be released with an annotation in the report that the matter was referred to the specific DCIO or Defense CI component. Notify the OCA, originator, and others as appropriate, after coordination with the DCIO or Defense CI component. If the DCIO or Defense CI component declines jurisdiction, the security inquiry or investigation shall continue. Annotate the report appropriately and include the identity of the

official who made the declination decision and his or her organization.

c. Coordination with OCA

(1) If the inquiry or investigation determines that a compromise occurred, the official initiating the inquiry or investigation shall immediately notify the originator (i.e., the OCA) of the information or material involved. The OCA(s) shall take the actions required by section 9 of this enclosure.

(2) If the originating activity no longer exists, the activity that inherited the functions of the originating activity shall be notified. If the functions of the originating activity were dispersed to more than one other activity, the inheriting activity(ies) cannot be determined, or the functions have ceased to exist, the senior agency official of the DoD Component of which the originating activity was a part shall be notified. This notification shall not be delayed pending completion of any additional inquiry or investigation or resolution of other related issues.

d. Security Inquiries. The head of the activity or activity security manager having security cognizance shall initiate an inquiry into the actual or potential compromise promptly to determine the facts and circumstances of the incident, and to characterize the incident as an infraction or a violation. At conclusion of the inquiry, a narrative of findings is provided in support of recommended additional investigative or other actions by the activity.

(1) The official appointed to lead the inquiry shall not be anyone involved with the incident. Preferably, the security manager should not be appointed to lead the inquiry.

(2) An inquiry shall be initiated and completed as soon as possible, not to exceed 10 duty days, and a report of findings provided to the activity head, activity security manager, and others as appropriate. If the inquiry cannot be completed within 10 duty days an extension should be requested from the appointing official.

(3) No recommendation should be made by an inquiry officer with regard to punitive action against the individual(s) responsible for the violation. An inquiry officer's function is to determine and report facts and make recommendations for actions needed to prevent future violations of the type investigated. Disciplinary or punitive action is the responsibility of the appropriate military commander or management official.

(4) If information obtained as a result of the inquiry is sufficient to provide answers to the following questions, then such information shall be sufficient to resolve the incident, to include instituting administrative sanctions consistent with section 17, Enclosure 3 of Volume 1 of this Manual.

(a) When, where, and how did the incident occur? What persons, situations, or conditions caused or contributed to the incident?

(b) Was classified information compromised?

(c) If a compromise occurred, what specific classified information and/or material was involved? What is the classification level of the information disclosed?

(d) If classified material is alleged to have been lost, what steps were taken to locate the material?

(e) Was the information properly classified?

(f) Was the information officially released?

(g) In cases of compromise involving the public media:

1. In what specific media article, program, book, Internet posting or other item did the classified information appear?

2. To what extent was the compromised information disseminated or circulated?

3. Would further inquiry increase the damage caused by the compromise?

(h) Are there any leads to be investigated that might lead to identifying the person(s) responsible for the compromise?

(i) If there was no compromise, and if the incident was unintentional or inadvertent, was there a specific failure to comply with established security practices and procedures that could lead to compromise if left uncorrected and/or is there a weakness or vulnerability in established security practices and procedures that could result in a compromise if left uncorrected? What corrective action is required?

e. Security Investigations. If the circumstances of an incident require a more detailed or additional investigation, then an individual shall be appointed by the activity head in writing, to conduct that investigation and, as appropriate, provide recommendations for any corrective or disciplinary actions.

(1) The individual appointed shall be sufficiently senior to ensure a successful completion of the investigation and should be commensurate with the seriousness of the incident; have an appropriate security clearance; have the ability to conduct an effective investigation; and shall be someone unlikely to have been involved, directly or indirectly, in the incident.

(2) Except in unusual circumstances, the activity security manager shall not be appointed to conduct the investigation.

(3) As an investigation may lead to administrative or disciplinary action, the evidence developed should be comprehensive in nature and gathered in such a manner that it would be admissible in a legal or administrative proceeding. Consult local legal counsel as needed for procedural guidance on conduct of the investigation.

(4) The investigation should be accomplished promptly following appointment of the investigating officer. The results of the investigation shall be documented in writing. The format in Appendix 1 to this enclosure may be used.

7. INFORMATION APPEARING IN THE PUBLIC MEDIA

a. If classified information appears in the public media, including on public Internet sites, or if approached by a representative of the media, DoD personnel shall be careful not to make any statement or comment that confirms the accuracy of or verifies the information requiring protection. Report the matter as instructed by the appropriate DoD Component guidance, but do not discuss it with anyone who does not, in the case of classified information, have an appropriate security clearance and need to know.

b. If the fact of an unauthorized public disclosure becomes widely know, the Component senior agency official should consider whether the workforce needs to be reminded of actions to be or not to be taken by individuals in response to the disclosure. Reminders may include such topics as not viewing or downloading the classified information from unclassified IT systems, not confirming the accuracy of the information, and providing a point of contact for media inquiries.

c. Notifications of unauthorized disclosures of classified information in the public media required by subparagraph 3.f.(1)(b) of this enclosure shall include the information specified in subparagraphs 7.c.(1) through 7.c.(7). Initial notifications providing basic information about the incident and a point of contact should be made as quickly as is feasible; complete information should be provided subsequently.

(1) Date, location, and author of the public media item.

(2) Specific information disclosed and its classification level.

(3) Identification of the OCA.

(4) The extent to which the disclosed information was circulated, both within and outside the Department of Defense, and the number of persons known to have had access to the information.

(5) An appraisal of or statement regarding the damage to national defense and/or national security programs caused by the disclosure.

(6) A statement of whether any investigative leads exist and what additional actions, if any, are contemplated (i.e., no further action; administrative investigation by the DoD Component; referral to the cognizant DCIO for criminal investigation; or a request for USD(I) referral to DoJ for investigation).

(7) Point of contact for further information.

d. When notified of a suspected compromise of classified information through the public media, the USD(I) shall, unless already done by the reporting DoD Component, consult with the Assistant Secretary of Defense for Public Affairs and other officials having a primary interest in the information to determine if the information was officially released under proper authority.

e. When responsibility for an inquiry into an unauthorized public media disclosure is unclear or is shared equally with another DoD Component, refer the matter through security channels to the USD(I) who shall decide investigative responsibility in consultation with the affected DoD Components.

f. The decision on whether to initiate an additional investigation by a DCIO or by the Federal Bureau of Investigation through a referral to the DoJ shall be based on the following factors:

(1) The accuracy of the information disclosed.

(2) The damage to national security caused by the disclosure and whether there were compromises regarding sensitive aspects of current classified projects, intelligence sources, or intelligence methods.

(3) The extent to which the disclosed information was circulated, both within and outside the Department of Defense, and the number of persons known to have access to it.

(4) The degree to which an investigation shall increase the damage caused by the disclosure.

(5) The existence of any investigative leads.

(6) The reasonable expectation of repeated disclosures.

g. If the DoD Component's initial inquiry or investigation or a DCIO investigation identifies the person(s) responsible for an unauthorized disclosure of classified information via the public media or Internet, the DoD Component shall notify the Director of Security, OUSD(I). This notification shall include responses to the DoJ Media Leak Questionnaire (see Appendix 2 of this enclosure). The USD(I), in coordination with the General Counsel of the Department of Defense (GC, DoD) and the Head of the DoD Component having OCA, shall decide whether additional investigation is appropriate and whether to refer the unauthorized disclosure to the DoJ for investigation and/or criminal prosecution. When the initial inquiry or investigation does not identify the person responsible, the Head of the DoD Component, in consultation with the USD(I) and the GC, DoD, shall decide if further investigation is appropriate.

8. RESULTS OF INQUIRIES AND INVESTIGATIONS

a. If the conclusion of the inquiry or investigation is that a compromise occurred and that weakness or vulnerability in established security practices and/or procedures contributed to the compromise or that the potential exists for a compromise of classified information due to a weakness or vulnerability in established security practices and/or procedures, the appropriate responsible security official shall take prompt action to issue new or revised guidance, as necessary, to resolve identified deficiencies. Results of inquiries and/or investigations into actual or potential compromises that indicate that defects in the procedures and requirements of this Manual contributed to the incident shall be reported to the Director of Security, OUSD(I).

b. If the conclusion of the inquiry or investigation is that a compromise did not occur, but that there was potential for compromise of classified information due to a failure of a person or persons to comply with established security practices and/or procedures, the official having security responsibility over such persons shall be responsible for taking action as may be appropriate to resolve the incident.

c. Additional investigation, beyond what is required by this enclosure, may be needed to permit application of appropriate sanctions for violation of regulations, criminal prosecution, or determination of effective remedies for discovered vulnerabilities. The inquiry this enclosure requires may serve as part of these investigations, but notifying OCAs shall not be delayed pending completion of these additional investigations.

9. ACTIONS TO BE TAKEN BY THE OCA. When notified of the compromise of classified information, the OCA shall:

a. Verify the classification and duration of classification initially assigned to the information.

b. Reevaluate the classification assigned to determine whether the classification shall be continued or changed. This classification review shall consider the following possibilities:

(1) The information has lost all or some of its sensitivity since it was initially classified and should be downgraded or declassified. (In rare cases, it might also be discovered that the information has gained sensitivity and should be upgraded.)

(2) The information has been so compromised by the incident that attempting to protect it further as classified is unrealistic or inadvisable, and it should be declassified.

(3) The information should continue to be classified at its current level.

c. Advise the activity reporting the compromise of the outcome of the classification assessment required by paragraphs 9.a and 9.b of this section within 72 hours of notification.

d. Assess the impact of the compromise on the affected system, plan, program, or project; consider countermeasures (e.g., damage control actions) that may be taken to minimize, mitigate or limit damage to national security and prevent further loss or compromise; and then initiate or recommend adoption of such countermeasures.

(1) Where appropriate, countermeasures should be applied as quickly as possible and may be initiated prior to completion of the classification review or damage assessment.

(2) Countermeasures could include changing plans or system design features, revising operating procedures, providing increased protection to related information (e.g., classification upgrading), or other appropriate actions.

(3) Evaluate the cost implications of information, operational, or technology losses; developmental and integration costs of countermeasures; likelihood of countermeasure success; and programmatic impacts of the unmitigated loss and/or compromise of specific classified information.

e. Conduct a damage assessment as required by section 10 of this enclosure to determine the effect of the compromise of classified information on the national security.

10. DAMAGE ASSESSMENTS

a. A damage assessment is undertaken to determine the effect of a compromise on the national security.

(1) A damage assessment shall normally consist of a detailed, multidisciplinary examination of the facts surrounding the compromise to determine the practical effects of a compromise on DoD programs, operations, systems, materials, and intelligence and on the Department of Defense's ability to conduct its missions; to address mitigations and countermeasures that could be put in place to decrease or offset the impact; to determine the estimated dollar costs to implement countermeasures essential to maintain or reinstate security, or to replace weapons systems or capabilities that are thoroughly compromised; and to provide, when appropriate, specific recommendations for action.

(2) A damage assessment is conducted after the classification review and often follows any prosecutorial actions. However, when necessary to identify damage done by the disclosure or otherwise appropriate, a damage assessment may be conducted pre-prosecution.

(3) The damage assessment is not to be confused either with the classification review performed by the OCA or with damage control actions, which are those actions performed immediately upon the discovery of disclosure or compromise to minimize risk, limit damage, and/or prevent further loss or compromise.

b. Each DoD Component shall establish a system of controls and internal procedures to ensure that damage assessments are conducted, at a minimum, for cases of compromise involving espionage, intelligence information or compromise via the public media. Damage assessments are encouraged for other compromises.

(1) Conduct of the damage assessment is the responsibility of the OCA and subject

matter experts. Security officials should provide assistance as needed and appropriate.

(2) The results of relevant security inquiries and investigations shall be made available to inform the damage assessment process, as needed. Reports of criminal or CI investigations associated with the compromise should be requested by the OCA from the cognizant DCIO or Defense CI component.

11. VERIFICATION, REEVALUATION, AND DAMAGE ASSESSMENT TIMELINES. The verification and reevaluation steps in section 9 of this enclosure, and when appropriate the damage assessment process in section 10 of this enclosure, shall be completed as soon as possible following notification of a compromise. However, damage assessments requiring multi-disciplinary or multiple agency review of the adverse effects of the compromise on systems, operations, and/or intelligence, may sometimes be a long-term process. The DoD goal for completion of a damage assessment involving compromised classified information is no longer than 6 months from the first date the compromise was declared. Accomplishment of the assessment prior to the initiation of legal or administrative proceedings may be beneficial; check with legal counsel.

12. ACTUAL OR POTENTIAL COMPROMISES INVOLVING MORE THAN ONE AGENCY. When classified information under the control of more than one DoD Component or another Federal agency is involved, the affected activities are responsible for coordinating their efforts in evaluating the classification of information involved and assessing damage.

13. DEBRIEFING IN CASES OF UNAUTHORIZED ACCESS. In cases where unauthorized access to classified information has occurred, it may be advisable to discuss the situation with the individual(s) to enhance the probability that he or she shall properly protect it. The activity head shall determine if a debriefing is warranted. This decision shall be based on the circumstances of the incident, what is known about the person(s) involved, and the nature of the information. The following general guidelines apply:

a. If the unauthorized access was by a person with the appropriate security clearance but no need to know, debriefing is usually appropriate only so far as necessary to ensure that the individual is aware that the information to which they had unauthorized access is classified and requires protection.

b. If the unauthorized access was by U.S. Government civilian or military personnel or an employee of a U.S. Government contractor, who does not have a security clearance, debriefing is usually appropriate. The person shall be advised of his or her responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if he or she fails to do so. The debriefing shall be designed to ensure that the individual understands the nature of the information, why its protection is important, and knows what to do if someone tries to obtain the information. In the case of non-DoD U.S. Government personnel and employees of U.S. Government contractors, the appropriate security official in the

individual's parent organization, including the appropriate facility security officer where applicable, shall be advised of the debriefing.

c. If the person involved is neither a member of a U.S. Government organization nor an employee of a U.S. Government contractor, the decision is much more situational. The key question is whether the debriefing shall have a positive effect on the person's ability or willingness to protect the information.

d. In any case where the person to be debriefed may be the subject of criminal prosecution or disciplinary action, consult with legal counsel before attempting to debrief the individual.

e. It is sometimes useful to have the person being debriefed sign a statement acknowledging the debriefing and his or her understanding of its contents, or to execute a SF 312. If an NDA is not executed, the nature and format of the statement is left to the discretion of the local security official to allow flexibility in meeting the requirements of a particular incident. If the person refuses to sign an NDA or debriefing statement when asked, this fact and his or her stated reasons for refusing shall be made a matter of record in the inquiry.

14. REPORTING AND OVERSIGHT MECHANISMS. The DoD Components shall establish necessary reporting and oversight mechanisms to ensure that inquiries and/or investigations are conducted when required, that they are done in a timely and efficient manner, and that appropriate management action is taken to correct identified problems. Inquiries or investigations and management analyses of security incidents shall consider possible systemic shortcomings that may have caused or contributed to the incident. The effectiveness of activity security procedures, security education, supervisory oversight of security practices, etc., shall be considered in determining causes and contributing factors. The focus of management response to security incidents shall be to eliminate or minimize the probability of further incidents occurring. Appropriate disciplinary action or legal prosecution, as discussed in section 17, Enclosure 3 of Volume 1 of this Manual, is sometimes one means of doing this, but the broader focus on prevention shall not be lost. Simple disciplinary action, without consideration of what other factors may have contributed to the situation, shall not be considered an acceptable response to a security incident.

Appendixes

1. Security Incident Reporting Format
2. DOJ Media Leak Questionnaire

APPENDIX 1 TO ENCLOSURE 6

SECURITY INCIDENT REPORTING FORMAT

1. The report format as described in Figure 2 is optional, to be used as a guide for appropriate content. The format may be used as shown or tailored to suit the organization and the circumstances. In all cases, the goal is to identify who, what, when, where, why, and how the incident occurred and to determine what should be done to preclude similar incidents in the future.
2. Classify, and appropriately mark, security incident reports according to content. At a minimum, reports shall be designated and marked “FOR OFFICIAL USE ONLY” as the reports will contain information on personnel involved. The reports may also contain other information that qualifies for designation as FOUO and information that could facilitate unauthorized access to classified information.

Figure 2. Report of Security Incident Inquiry or Investigation

TO: Official Initiating Inquiry or Investigation (e.g., Activity Security Manager or Activity Head) (others as required)

THRU: (Appropriate chain of command)

SUBJECT: Report of Security Incident Inquiry or Investigation

1. Summary: A summary of who, what, when, where, why, and how the violation occurred. (Also see DoD Manual 5200.01-V3, section 6 of Enclosure 6.)

2. Sequence of Events: A detailed sequence of events tracing the security violation from start to finish. This sequence will include a list of all personnel (include name, grade, social security number (for positive identification and adverse information reporting), position, organization, clearance level, and access authorized) involved in order of their specific time of involvement; and all locations involved.

a. Indicate date of violation's discovery and likely occurrence (if known). Identify the material (e.g., documents, information, or equipment) involved in the violation. Identify individuals not cleared for classified information and the extent of exposure. Identify procedural problems or other factors that may have contributed to the violation.

b. Provide a detailed description of the information involved in the incident. Include classification, compartment levels, caveats and any control or dissemination notices; identification of the material (e.g., message, letter, staff study, imagery, magnetic media, equipment item) by subject and date or nomenclature, to include any control/serial numbers; originating office and OCA; and volume of material (e.g., number of pages or items of equipment) involved.

c. Make a statement as to the likelihood of compromise. If material has been compromised, identify the extent of compromise and state the date or time period during which information was lost or compromised. Identify by name the individual(s) and organization(s) of personnel at fault for, or contributing to, the violation, if possible, and reason(s) they are culpable or contributed to the occurrence of a violation.

d. Identify deficient procedure(s) and describe how they led or contributed to the incident (too vague, weak, out-of-date, unenforceable, ineffective, etc.). Include any assessment regarding systemic weaknesses or vulnerabilities in established security practices (e.g., non-existent, out-of-date, or ineffective policies, procedures or training) that must be corrected; suggest the corrective actions required.

3. Actions taken: List actions that have been taken (e.g., notifications made, messages sent, interviews with, counseling of, and discipline rendered for individuals involved, and other information as required). Include dates inquiry or investigation started and ended.

4. Recommendations: Make recommendations concerning what should be done to preclude future incidents of this type.

5. Identification of inquiry or investigating official, organization, and telephone numbers.

6. Evaluation notes. Enter other information relevant to the inquiry or investigation. Attach interview statements and/or records, documentary evidence, exhibits and so forth, as appropriate.

(Signature of Inquiry or Investigating Official)

FOR OFFICIAL USE ONLY (or, if classified, insert classification and add other markings as required)

APPENDIX 2 TO ENCLOSURE 6

DOJ MEDIA LEAK QUESTIONNAIRE

If the initial inquiry and/or investigation into an unauthorized disclosure of classified information via the media identifies the person responsible for the unauthorized disclosure, the Head of the DoD Component shall promptly answer to the fullest extent possible the standard questions in this appendix, which comprise the DoJ Media Leak Questionnaire, and submit the questionnaire through security channels to the USD(I). In coordination with the GC, DoD, the USD(I) shall, when warranted, forward the information via letter to:

Department of Justice, Criminal Division
Attention: Chief, Internal Security Section
Bond Building, Room 9400
1400 New York Avenue, NW
Washington, DC 20530

- a. What is the date and identity of the media source (e.g., article, blog, television, or other oral presentation) containing classified information?
- b. What specific statement(s) in the media source are classified and was the information properly classified?
- c. Is the classified information disclosed accurate?
- d. Did the information come from a specific document, and if so, what is the origin of the document and the name of the individual responsible for the security of the classified data discussed?
- e. What is the extent of official circulation of the information?
- f. Has the information been the subject of prior official release?
- g. Was prior clearance for publication or release of the information sought from proper authorities?
- h. Has the material, parts thereof or enough background data, been published officially or in the press to make an educated speculation on the matter possible?
- i. Will the information be made available for use in a prosecution, and if so, what is the name of the person competent to testify on its classification?
- j. Was declassification considered or decided on before the data appeared in the media?
- k. What effect might the disclosure of the classified data have on the national defense?

ENCLOSURE 7

IT ISSUES FOR THE SECURITY MANAGER

1. OVERVIEW. This enclosure identifies and discusses the most common IT issues facing security organizations and provides references and pointers to the relevant primary sources. As the Internet, classified and unclassified networks, and a wide range of computer systems are used in every facet of the operation of the Department of Defense, challenges and questions related to IT issues and the interaction between the security and IT staffs abound. The traditional security manager's portfolio, planning horizon, and focus on classification management and personal, physical, and operational security issues no longer suffice. The continuing protection and security of complex IT and information systems depends upon a robust and effective interaction and coordination between security and IT organizations.

2. RESPONSIBILITY. In accordance with Reference (b), overall security responsibility for protection of classified information and CUI remains with the information security program and staff, even though the data and/or information resides on IT and information systems and networks managed and controlled by the DoD Component Chief Information Officer. Accordingly, proactive and continuous engagement and collaboration between security, IT, and IA professionals, at all organizational levels, is essential in order to ensure the protection of DoD information as well as the Department's electronic enterprise.

3. IA ROLES AND FUNCTIONS

a. In accordance with Reference (v) and DoDD 8000.01 (Reference (bs)), IA and IT policy and information systems operations are the purview of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO) at the OSD level and the counterpart organizations in the DoD Components.

b. U.S. Strategic Command, through U.S. Cyber Command (USCYBERCOM), has the overall responsibility for directing the operation of and assuring the security of the global DoD network environment. USCYBERCOM will lead the day-to-day defense and protection of the DoD networks and will coordinate all DoD network operations, providing full spectrum support to military and counterterrorism missions.

c. At the DoD Component and activity level, there are several important IA roles and functions that security managers need to recognize and understand to develop a productive relationship with the IA staff, including the designated approving authority (DAA), IAM, and IA officer (IAO). The Glossary provides definitions of these functions and identifies other titles that are sometimes used for these same functions.

4. IA CONCEPTS

a. IA Attributes. All DoD information systems are to maintain appropriate levels of availability, integrity, authentication, confidentiality, and non-repudiation in order to protect and defend DoD information and networks. While all five of these attributes are critical to the user's ability to perform the assigned mission, from an information security perspective, confidentiality and authentication may be the most important.

(1) The loss of availability means that the information system, computer network, and/or data are unavailable to authorized users, and missions or operations cannot be performed. Loss of availability within a computing environment may be an extremely serious event, depending on the criticality of the applications and missions supported.

(2) The loss of integrity means that the data can no longer be trusted to be reliable or accurate.

(3) Authentication is critical, as it is the mechanism that authorizes or allows access to computer systems and networks and the data that resides there. Loss of or incorrect authentication services could allow unauthorized access to classified data.

(4) The loss of confidentiality means that data may be available in an electronic form to users who are not authorized to receive it. Depending on the classification level of the system or network, loss of confidentiality could mean a compromise of classified information.

(5) The loss of non-repudiation assurances means that authorized users no longer can be certain with whom they are communicating because general communications (and therefore the data processed by that information system) cannot be trusted or verified.

b. System Categorization. Each information system must be categorized and have appropriate IA controls assigned in accordance with Reference (bf). System categorization requires determination of the potential impacts of the loss of confidentiality, integrity, and availability associated with the specific system or information. IA controls are selected based on the results of the system categorization process. Security personnel may find it helpful to understand the categorization of the DoD information system(s) within their area of responsibility, as those designations impact the information, physical, personal, and operational security environment and the resource requirements that must be dedicated to protection of the system(s) and the information processed.

c. Certification and Accreditation (C&A). C&A of DoD systems is governed by Reference (s).

(1) Certification is the comprehensive evaluation of the technical and nontechnical (e.g., procedural) security safeguards of an information system undertaken to support the accreditation process. It establishes the extent to which a particular design and implementation meets a set of specified security requirements.

(2) Accreditation is the formal declaration by a DAA that, based on the implementation

of a specified set of technical, managerial, and procedural safeguards, the level of risk is acceptable and the information system is approved to operate at a specific security level.

(3) The security manager and the DAA should coordinate with each other during the C&A process. The DAA needs to work with the security organization to ensure an understanding of the security requirements that must be met based on the classification of the information to be processed, and for identification of any security issues associated with the operation of the system. The security staff, on the other hand, must be aware of the nature, scope, and schedule of ongoing C&A activities within a given organization, in order to provide timely and relevant classification management direction and to ensure the physical environment is properly secured and accredited for the operations planned and that users are properly cleared and have all requisite access in time to support the mission.

5. DATA SPILLS

a. Classified data spills occur when classified data is introduced either onto an unclassified information system or to an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category. Although it is possible that no unauthorized disclosure occurred, classified data spills are considered and handled as a possible compromise of classified information involving information systems, networks, and computer equipment until the inquiry determines whether an unauthorized disclosure did or did not occur.

b. When a classified data spill occurs, the activity security manager is responsible ensuring that the policy requirements for addressing an unauthorized disclosure, as specified in Enclosure 6 or other provisions of this Manual, are met (e.g., inquiry, notification, investigation, damage assessment); however, these responsibilities must be carried out in close coordination with the IT and/or IA staff, which has overall responsibility for the operation of the networks and systems as well as the technical knowledge needed to address the spill. Security personnel have the overall lead for addressing such events.

c. CNSS Policy 18 (Reference (bt)) applies to the spillage of classified national security information on any information system, be it government, contractor, or privately owned, and provides a policy framework for the consistent handling of the spillage. Each Federal Government organization that owns or operates classified information systems is required to establish policies and procedures for handling classified information spillage. When a classified data spill occurs, Reference (bt) requires that it is immediately:

(1) Reported to the appropriate authorities, including, at a minimum, the OCA, the information owner/originator, the IAM, the activity security manager, and the responsible computer incident response center.

(2) Isolated and contained to minimize damage and to preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or CI purposes. All affected media is to be considered classified at the same level as the spilled information until the appropriate remediation processes have been executed and verified.

(3) Verified to be classified by the information owner, who shall also ensure an assessment is conducted, as appropriate, in accordance with References (d) and (f) and this Manual.

d. CNSS Instruction 1001 (Reference (bu)) implements Reference (bt) and provides a list of questions that should be asked when investigating a spill, potential options for remediating the effects of a spill, and factors to be considered in selecting a remediation procedure.

e. Information concerning a classified spillage incident shall be protected from disclosure. Communications regarding the fact that a spill situation exists should be communicated to those involved, including the remediation teams, via secure communications whenever possible. The technical remediation teams must be cleared to the level of the information that may have been spilled.

f. Decisions regarding mitigation procedures, including disposition of affected media (i.e., sanitization, physical removal, or destruction) shall realistically consider the potential harm that may result from compromise of spilled information.

g. During a spill event, a speedy and coordinated response among security, IA, and other technical personnel is vital. Significant unauthorized or inadvertent dissemination of classified information on unclassified information systems can occur rapidly.

(1) Once a spill is reported, the information system support organization must, whenever possible, quickly implement technical isolation of contaminated workstations, servers, and back-up systems to avoid spreading the contamination, to avoid loss of systems availability, and to minimize exposure of classified information to those individuals or organizations not authorized to receive it. At the same time, the security and IT staffs must begin the process of determining whether a security incident has actually occurred. If so, remediation procedures, which must be developed, approved, and tested in advance, should be implemented.

(2) E-mail (whether in the body of the e-mail or attachment) is the most common method by which spills occur. The IA staff should have proven procedures to remediate up to Secret-level spills to portable computing devices. Remediation of Top Secret, SAP, and SCI spills to personal electronic devices (PED), however, may entail destruction of the hardware.

(3) For Secret-level spills and below, the technical state of the art currently allows for overwriting and sanitization of contaminated media, and reentry of the media into service. There is no approved overwriting or sanitization procedure for media that has been contaminated with Top Secret, SAP, or SCI data, short of physical destruction. However, such media may continue to be used if (re)classified at the higher level, where appropriate.

(4) Early identification of classified spills, and a thorough understanding of where the spilled data was sent, is essential to avoid widespread contamination (or re-contamination) of back-up servers, tape systems, and off-site storage locations, most of which are configured to run nightly or during periods of low usage.

h. Classified spills to a personally owned device should also be reported to security officials immediately so remediation can be undertaken as necessary to prevent further unauthorized disclosure.

6. DISPOSAL OF COMPUTER MEDIA

a. NSA/CSS publishes lists of products that meet specific performance criteria for sanitizing, destroying or disposing of various types of media containing sensitive or classified information. Among the products identified are those that can be used for erasure of magnetic storage devices (e.g., hard drives) and destruction of optical media (e.g., CDs and DVDs). The lists are available at http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml or by calling (410) 854-6358. The NSA/CSS Storage Device Declassification Manual, available at that web address, addresses procedures required for sanitization, declassification and release of computer storage devices that have held classified information. Overwriting as a method of clearing previously classified data may be used when the media is reused within the same environment. Sections 17 and 18 of Enclosure 3 of this Volume provide additional guidance on destruction of classified information.

b. When no longer needed, UNCLASSIFIED computer systems and hard drives may be disposed of outside the Department of Defense. In some circumstances, the equipment may be provided to non-government entities for reutilization. To ensure that no data or information remains on operable unclassified hard drives that are transferred or permanently removed from DoD custody, the drives must be sanitized by overwriting. Where overwriting is inappropriate or cannot be accomplished (e.g., inoperable disk) or the drives are to be totally removed from service (i.e., thrown away), the drives must be destroyed. The specific methods and procedures differ depending on sensitivity of data and ownership of the hard drive. To ensure DoD information is not inadvertently disclosed to unauthorized individuals, the activity security manager should coordinate with the local DAA and/or IT staff to ensure local procedures for disposal of computer hard drives appropriately address removal of U.S. Government data prior to disposal. (See Assistant Secretary of Defense for Command, Control, Communications and Intelligence Memorandum (Reference (bv)) for detailed guidance.)

7. NON-TRADITIONAL WORK ENVIRONMENTS. Increasingly, a wide variety of sensitive and even classified activities are performed from non-traditional work environments, to include employee homes. In the historic context, this work has principally involved unclassified information and projects. However, classified IT (e.g., SIPRNET) systems and installations are increasingly being approved for utilization by senior personnel. When such is the case, in addition to the requirements of section 12 of Enclosure 2 of this Volume, the following minimum physical and administrative security criteria must be addressed:

a. Physical site security survey/analysis. Where prudent, a crime survey may be requested from local authorities to facilitate understanding of risks associated with the site.

b. Employee training on classified information systems operation, as well as protection and storage of classified information and COMSEC materials.

c. Provisions for secure storage and/or destruction of any classified information that may be required or generated (e.g. storage of COMSEC key materials, classified hard drives, and documents).

d. Application of and compliance with requirements for security-in-depth.

e. Written approval for such use of classified information and equipment.

8. REQUIREMENT FOR ENCRYPTION OF CERTAIN UNCLASSIFIED DATA. In accordance with DoD policy, all unclassified DoD data that has not been approved for public release and is stored on mobile computing devices or removable storage media must be encrypted using commercially available encryption technology. This requirement includes all CUI as well as other unclassified information that has not been reviewed and approved for public release. See ASD(NII) Memorandum (Reference (bw)) for detailed guidance.

9. PII

a. PII, which is a type of CUI, must be protected from public disclosure in accordance with Federal policy, as described in ASD(NII) Memorandum (Reference (bx)) and Director, Administration and Management Memorandum (Reference (by)). Some PII also qualifies for protection under the provisions of section 552a of Reference (bm) (also known and hereinafter referred to as “The Privacy Act of 1974, as amended”). Certain PII requires data-at-rest encryption and other protections.

b. PII has protection and reporting requirements of which the activity security manager should be aware in the event the loss or unauthorized disclosure of PII (known as a “breach”) is reported to the security office, separately or as part of an unauthorized disclosure of classified information. Although Privacy Act and/or IT officials are responsible for addressing a breach, activity security managers should be familiar with the protection and breach reporting requirements, the required timeframes for such reports, and the process identified in the DoD Component breach remediation plan for responding to breaches. A breach may trigger a chain of required actions, including notifications to the USCYBERCOM, United States Computer Emergency Readiness Team, the DoD Component Head, and DoD Privacy Act officials. Breach reports must be unclassified.

10. NEW TECHNOLOGY AND EQUIPMENT. Technology, in general, and IT technology specifically, changes much more quickly than information security policy. New products for data storage, communications, access control, and intrusion detection, and new IT equipment and peripherals (e.g., hand-held classified devices such as the Secure Mobile Environment PED (commonly referred to as “SME PED”)) all have implications, and potential challenges, for

information security. The security manager must remember that the fundamental principles upon which the information security program resides are still applicable and provide the foundation for dealing with new capabilities. The activity security manager must work with the IAM and the local DAA(s) to identify new risks and develop appropriate procedures to mitigate those risks. Where new policy or procedures are required to address new capabilities, suggested updates and/or issues should be forwarded through the security chain of command to the Director of Security, OUSD(I).

11. INTERNET-BASED SOCIAL NETWORKING SERVICES. Use of Internet-based social networking services, such as Facebook, Twitter, YouTube, and MySpace, is governed by Directive-Type Memorandum 09-026 (Reference (bz)). The policy addresses both official use of such capabilities and non-official use by DoD personnel. It also covers use of other publicly accessible information capabilities and applications available on the Internet (e.g., wikis, blogs) in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. As each DoD Component is responsible for ensuring all uses of these services are compliant with information security, IA and OPSEC policies and procedures, officials from these disciplines need to coordinate efforts to implement appropriate training, procedures, and oversight. The requirements for protecting classified information and CUI from unauthorized disclosure are the same when using social networking services as when using other media and methods of dissemination and the penalties for ignoring the requirements are likewise the same.

12. MARKING REQUIREMENTS FOR ELECTRONIC INFORMATION. Regardless of media, the requirement to identify as clearly as possible the information requiring protection remains. Where it is not feasible to include markings with all of the information required for classified documents, an explanatory statement that provides the required information shall be included on the item or with the documentation that accompanies it.

a. For specific guidance on marking in an electronic environment, see section 17, Enclosure 3 of Volume 2 of this Manual, as well as related information in section 16 (briefing slides) and paragraph 18.g (removable electronic storage media) of the same enclosure.

b. The use of metadata and other electronic tags, as required by DoDD 8320.02 (Reference (ca)), to identify the classification level, releasability, and other security attributes of electronic data files can facilitate automated application and enforcement of security measures. However, it is imperative that metadata and electronic tags associated with declassified or downgraded information in electronic format be reviewed and updated or deleted, as necessary, to reflect the actual classification and other attributes of the information. Precautions must be taken to ensure classified attributes are not released with unclassified data.

13. PROCESSING REQUIREMENTS FOR SPECIFIC TYPES OF INFORMATION

a. SCI. SCI, regardless of classification level, must be processed only on an information system accredited for SCI processing (e.g., Joint Worldwide Intelligence Communications

System (JWICS)). It may not be processed on, transferred to, or stored on SIPRNET, even if the information is SECRET//SI, SECRET//HCS, etc., as SIPRNET is not accredited for SCI. Any transfer to and/or processing of SCI on SIPRNET constitutes a data spillage from a higher to a lower-security information domain, in accordance with Reference (bt).

b. RD and Critical Nuclear Weapons Design Information (CNWDI). RD and CNWDI require certain access and dissemination controls, as specified by DoDI 5210.02 (Reference (cb)), beyond those for other information of a comparable level of security classification. Requirements for processing RD or CNWDI are specified in section 12, Enclosure 3 of Volume 1 of this Manual.

c. SAP. SAP information, regardless of classification, shall be processed only on an information system specifically accredited for SAP processing and operating at a classification level that meets or exceeds the classification level of the SAP data.

d. Controlled Imagery. Information marked "IMCON" (controlled imagery) may not be processed on SIPRNET or posted to SIPRNET websites without prior approval from the National Geospatial-Intelligence Agency. See Appendix 2, Enclosure 4 of Volume 2 of this Manual.

e. NATO Information. NATO information, regardless of classification, must be processed on U.S. government CLASSIFIED information systems operating at an appropriate level of classification with encrypted data transport and storage and specifically accredited for NATO processing, in accordance with the requirements of Reference (ac) and Deputy Secretary of Defense Memorandum (Reference (cc)). For further guidance on accreditation, handling and processing of NATO information, including how to handle data spills involving NATO information, contact the Central U.S. Registry.

f. CUI. FOUO and other CUI may NOT be posted to publicly-accessible Internet sites and may NOT be posted to sites whose access is controlled only by domain (e.g., limited to .mil and/or .gov) as such restricted access can easily be circumvented. At a minimum, posting CUI to a website requires certificate-based (e.g., common access card) or password and ID access as well as encrypted transmission using hypertext transfer protocol secure (https) or similar technology. CUI other than FOUO may have additional posting restrictions. See Deputy Secretary of Defense Memorandum (Reference (cd)) for detailed guidance.

14. COMPILATION AND DATA AGGREGATION. The ability to create large databases as well as nearly universal Internet posting of information makes use of search, data mining, and other data correlation tools convenient and easy. All of these capabilities facilitate creation of classified compilations of data. The security manager should consider the potential for creation of classified compilations when reviewing Internet postings, new IT systems, and security classification guides, and, as appropriate, when other classification assistance is requested. See Enclosure 4 of Volume 1 of this Manual, for guidance on classification by or as a result of compilation and Enclosure 6 of Volume 1 for considerations relative to Internet posting of data elements known to comprise classified compilations.

GLOSSARYPART I. ABBREVIATIONS AND ACRONYMS

AC	alternating current
ACCM	alternative compensatory control measures
AECS	automated entry control systems
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
AUS	Australia
C&A	certification and accreditation
CD	compact disc
CFR	Code of Federal Regulations
CI	counterintelligence
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CNSS	Committee on National Security Systems
CNWDI	Critical Nuclear Weapon Design Information
COMSEC	communication security
CONUS	continental United States
CPI	critical program information
CUI	controlled unclassified information
DAA	designated approval authority
DC	direct current
DCIO	defense criminal investigative organization
DCS	Defense Courier Service
DD	DoD
DGR	designated government representative
DMS	Defense Message System
DNI	Director of National Intelligence
DoDD	DoD Directive
DoDI	DoD Instruction
DoJ	Department of Justice
DSA	designated security authority
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence and Security
DVD	digital video disc (also digital versatile disc)
E.O.	Executive Order
FED-STD	Federal Standard
FGI	foreign government information
FMS	foreign military sales
FOUO	For Official Use Only
FRD	Formerly Restricted Data

GAO	Government Accountability Office
GC, DoD	General Counsel of the Department of Defense
GPO	Government Printing Office
GSA	General Services Administration
HUMINT	human intelligence
IA	information assurance
IAM	information assurance manager
IAO	information assurance officer
ID	identification
IDE	intrusion detection equipment
IDS	intrusion detection system
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
IT	information technology
JPAS	Joint Personnel Adjudication System
JWICS	Joint Worldwide Intelligence Communications System
LOA	letter of offer and acceptance
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NCIX	National Counterintelligence Executive
NDA	non-disclosure agreement
NOFORN	not releasable to foreign nationals
NSA/CSS	National Security Agency/ Central Security Service
NTISSI	National Telecommunications Information Systems Security Instruction
OCA	original classification authority
ODNI	Office of the Director of National Intelligence
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
OUSD(P)	Office of the Under Secretary of Defense for Policy
PCU	premise control unit
PED	personal electronic device
PII	personally identifiable information
PIN	personal identification number
POE	port of embarkation
RD	Restricted Data
REL TO	authorized for release to

SAP	Special Access Program
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SF	standard form
SIPRNET	Secret Internet Protocol Router Network
SPECAT	Special Category
TSA	Transportation Security Administration
TSCM	technical surveillance countermeasures
UK	United Kingdom
UL	Underwriters Laboratories
U.S.C.	United States Code
USCYBERCOM	U.S. Cyber Command
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Manual.

access. The ability or opportunity to obtain knowledge of classified information.

activity head. See “heads of DoD activities.”

activity security manager. The individual specifically designated in writing and responsible for the activity’s information security program which ensures that classified information and CUI is properly handled during its entire life cycle. This includes ensuring it is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken. The security manager may be assigned responsibilities in other security disciplines such as personnel and physical security, etc.

agency. Any “Executive Agency” as defined in section 105 of Reference (bm); any “Military Department” as defined in section 102 of Reference (bm); and any other entity within the Executive Branch that comes into the possession of classified information.

alarmed zone. The totality of area covered by a premise control unit and the sensors it serves.

Australian Communities. The Australian Government entities with facilities and non-governmental facilities identified on the Department of State’s Directorate of Defense Trade Controls website (<http://www.pmdtcc.state.gov/treaties/index.html>) at the time of export.

authentication. Those measures designed to establish the validity of attributes associated with some entity (e.g., user, process, or device), or a means of verifying an individual's authorization to receive specific categories of information. Authentication is often accomplished as a prerequisite to allowing access to resources in an information system.

authorized person. A person who has a favorable determination of eligibility for access to classified information, has signed a SF 312, and has a need to know for the specific classified information in the performance of official duties.

automated information system. An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

automatic declassification. The declassification of information based solely upon:

The occurrence of a specific date or event as determined by the OCA; or

The expiration of a maximum time frame for duration of classification established pursuant to Reference (d).

availability. Timely, reliable access to data and information services for authorized users.

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

classified national security information. Information that has been determined pursuant to Reference (d), or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

classifier. An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an OCA or a person who derivatively assigned a security classification based on a properly classified source or a security classification guide.

collateral information. All national security information classified Confidential, Secret, or Top Secret under the provisions of an E.O. for which special systems of compartmentation (such as SCI or SAP) are not formally required.

COMSEC. The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes crypto security, emission security, transmission security, and physical security of COMSEC material and information.

compromise. An unauthorized disclosure of classified information.

confidentiality. Assurance that information is not disclosed to individuals, devices, processes, or other entities unless they have been authorized access to the information.

CONUS. U.S. territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

CPI. Defined in DoDI 5200.39 (Reference (ce)).

DAA. The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

damage assessment. A formal multi-disciplinary analysis to determine the effect of a compromise of classified information on the national security

damage to the national security. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

declassification. The authorized change in the status of information from classified information to unclassified information.

declassification authority. The official who authorized the original classification, if that official is still serving in the same position;

The originator's current successor in function;

A supervisory official of either; or

Officials delegated declassification authority in writing by the agency head or the senior agency official.

declassification guide. Written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified. Also a guide providing classification and declassification instructions specifically for information that is 25 years old or older and of permanent historical value. A declassification guide is the most commonly used vehicle for obtaining ISCAP approval of 25-year exemptions from the automatic declassification provisions of Reference (d).

defense articles. For purposes of the Defense Trade Cooperation Treaty between the United States and Australia or the United Kingdom, those articles, services, and related technical data, including software, in tangible or intangible form, listed on the United States Munitions List of Reference (y). Defense articles exempt from the scope of section 126.17 of Reference (y) are identified in Supplement No. 1 to Part 126 of Reference (y).

derivative classification. Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification

distribution statement. A statement used on a technical document to denote the extent of its availability for secondary distribution, release, and disclosure without additional approvals or authorizations. A distribution statement marking is distinct from and in addition to a security classification marking. A distribution statement is also required on security classification guides submitted to DTIC.

document. Any recorded information, regardless of the nature of the medium or the method or circumstances of recording. This includes any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage media.

downgrading. A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

escort. A cleared individual who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort, but the conveyance in which the material is transported remains under the constant observation and control of the escort.

espionage. Those activities designed to obtain, deliver, communicate, or transmit information relating to the national defense with the intent or reason to believe such information will be used to the injury of the United States or to the advantage of a foreign nation or transnational entity.

exempted. Nomenclature and marking indicating information has been determined to fall within an enumerated exemption from automatic declassification in accordance with Reference (d).

FGI

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.

Information produced by the U.S. Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

Information received and treated as “Foreign Government Information” pursuant to the terms of a predecessor order to Reference (d).

FRD. Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as Restricted Data.

FOUO. A protective marking to be applied to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more provisions of the FOIA. This includes information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended. See DoD 5400.7-R (Reference (cf)) for detailed information on categories of information that may qualify for exemption from public disclosure.

heads of DoD activities. Heads, either military or civilian, of organizations, commands, and staff elements subordinate to a DoD Component, with jurisdiction over and responsibility for the execution of the organization's mission and functions, including its information security program. The official may variously carry the title of commander, commanding officer, or director, or other equivalent title.

homeland. The physical region that includes the continental United States, Alaska, Hawaii, United States possessions and territories, and surrounding territorial waters and airspace.

IAM. The individual responsible for the IA program of a DoD information system or organization. While the term IAM is favored within the Department of Defense, it may be used interchangeably with the title information systems security manager.

IAO. An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization. While the term IAO is favored within the Department of Defense, other titles also are used (e.g., information systems security officer, information systems security custodian, network security officer, or terminal area security officer).

information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

information security. The system of policies, procedures, and requirements established in accordance with Reference (d) to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures and requirements established to protect controlled unclassified information, which may be withheld from release to the public in accordance with statute, regulation, or policy.

infraction. Any knowing, willful, or negligent action contrary to the requirements of Reference (d), its implementing directives, or this Manual that does not constitute a "violation," as defined herein.

inquiry. The initial fact-finding and analysis process to determine the facts of any security incident.

integrity. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed. Integrity in the IA environment addresses the logical correctness, completeness, and reliability of the operating system, and the system hardware, software and data. In a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of data or information.

Intelligence Community. An element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended (Reference (cg)), or section 3.5(h) of E.O. 12333 (Reference (ch)).

international program. Any program, project, contract, operation, exercise, training, experiment, or other initiative that involves a DoD Component or a DoD contractor and a foreign government, international organization, or corporation that is located and incorporated to do business in a foreign country.

investigation. An in-depth, comprehensive examination of the facts associated with a security violation.

loss. The inability to physically locate or account for classified information.

material. Any product or substance on or in which information is embodied.

metadata. Structured information that describes, explains or locates data or otherwise makes data easier to retrieve, use or manage. Metadata captures or specifies basic attributes and characteristics about information and is often referred to as information about information. Typical metadata in an electronic environment includes such attributes as author, creation date, file size, and storage location. Security metadata may include attributes such as classification level, OCA, and date for declassification.

national security. The national defense or foreign relations of the United States. National security includes defense against transnational terrorism.

need to know. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

network. A system of two or more computers that can exchange data or information.

nickname. A nickname is a combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

non-repudiation. The condition where the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

open storage area. An area constructed in accordance with the requirements of the Appendix to Enclosure 3 of this Volume and authorized by the senior agency official for open storage of classified information.

original classification. An initial determination that information requires, in the interests of national security, protection against unauthorized disclosure.

OCA. An individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to originally classify information (i.e., to classify information in the first instance).

permanent historical value. Having sufficient value to warrant being maintained and preserved permanently.

PII. Unique information about an individual that can be used to distinguish or trace his or her identity. It includes, but is not limited to, name, social security number, date and place of birth, mother's maiden name, home address and phone number, personal e-mail address, biometric records, financial transactions, medical history, criminal or employment history, and other information to which a security manager may have access. PII does not include an individual's name when it is associated with work elements, such as duty phone number, duty address, and U.S. Government e-mail address.

protective security service. Defined in DoD 5220.22-C (Reference (ci)).

public media. A medium of communications designed to reach the public. Public media includes print media (e.g., newspapers, magazines, books), broadcast media (e.g., radio, television) and Internet media (e.g., websites, blogs, tweets).

records. The records of an agency and Presidential papers or Presidential records, as those terms are defined in chapters 22 and 33 of Reference (t), including those created or maintained by a U.S. Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

records management. The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. Within the Department of Defense, records management is implemented by Reference (u).

RD. All data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but not data declassified or removed from the Restricted Data category pursuant to section 2162 of The Atomic Energy Act of 1954, as amended (Reference (cj)).

safeguarding. Measures and controls that are prescribed to protect classified information.

SAP. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. In the Department of Defense, any DoD program or activity (as authorized in Reference (d)), employing enhanced security measures (e.g., safeguarding, access requirements, etc.), exceeding those normally required for collateral information at the same level of classification, shall be established, approved, and managed as a DoD SAP in accordance with Reference (ah).

SCI. Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of National Intelligence.

secure room. An open storage area.

security classification guide. A documentary form of classification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

security clearance. A determination that a person is eligible in accordance with the standards of Reference (l) for access to classified information.

security-in-depth. A determination by the senior agency official that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an IDS, random guard patrols throughout the facility during non-working hours, closed circuit video monitoring or other safeguards that mitigate the vulnerability of open storage areas without alarms and security containers during non-working hours.

self-inspection. The internal review and evaluation of individual DoD Component activities and the DoD Component as a whole with respect to the implementation of the program established in accordance with References (b), (d), and (f), and this Manual.

senior agency official. An official appointed by the Head of a DoD Component to be responsible for direction, administration, and oversight of the Component's Information Security Program, to include classification, declassification, safeguarding, and security education and training programs, and for the efficient and effective implementation of References (b), (d), (e), and (f) and the guidance in this Manual. Where used in reference to authorities under section 5.4(d) of

Reference (d), this term applies only to the Senior Agency Officials of the Military Departments and of the Department of Defense.

telecommunications. The preparation, transmission, or communication of information by electronic means.

unauthorized disclosure. Communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient.

United Kingdom Communities. The UK Government entities with facilities and non-governmental facilities identified on the Department of State's Directorate of Defense Trade Controls website (<http://www.pmddtc.state.gov/treaties/index.html>) at the time of export.

United States and its territories. The 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the United States Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and Northern Mariana Islands.

vault. An area approved by the Head of the DoD Component which is designed and constructed of masonry units or steel lined construction to provide protection against forced entry and which is equipped with a GSA-approved vault door and lock. A modular vault approved by the GSA may be used in lieu of a vault.

violation. Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; or

Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of Reference (d), its implementing directives, or this Manual; or

Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of Reference (d), Reference (ah), or this Manual.