APPENDIX 15

DoD Manual 5200.01-V3 Information Security

Department of Defense

MANUAL

NUMBER 5200.01, Volume 3
February 24, 2012
Incorporating Change 1 March 21, 2012

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 is effective upon its publication to 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

(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, 1981[1]
(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 2006[2]
(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, 2007[3]
(ad) Department of Defense and United Kingdom Ministry of Defense, "Security Implementing Arrangement," January 27, 2003[4]
(ae) Chairman of the Joint Chiefs of Staff Manual 3150.29C, "Code Word, Nickname, and Exercise Terms Report (NICKA) System," December 7, 2007[5]
(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, 2005[6]
(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 edition[7]
(al) Federal Standard 832, "Construction Methods and Materials for Vaults," September 1, 2002[7]
(am) Federal Specification FF-L-2937, "Combination Lock, Mechanical," January 31, 2005, as amended[7]
(an) Federal Specification AA-F-358, "Filing Cabinet, Legal and Letter Size, Uninsulated, Security," current edition[8]
(ao) Federal Specification AA-V-2737, "Modular Vault Systems," April 25, 1990, with Amendment 2, October 30, 2006[7]
(ap) Federal Specification FF-P-110, "Padlock, Changeable Combination (Resistant To Opening By Manipulation and Surreptitious Attack)," current edition, as amended[7]
(aq) Section 1386 of title 18, United States Code
(ar) Federal Standard 809, "Neutralization and Repair of GSA Approved Containers and Vault Doors," current edition[7]

---

[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

(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, 1993[7]
(av) Underwriters Laboratories Inc., Standard 634, "Standard for Connectors and Switches for Use with Burglar-Alarm Systems," October 12, 2007[9]
(aw) National Security Agency/Central Security Service Policy Manual 3-16, "Control of Communications Security (COMSEC) Material," August 2005[10]
(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, 2008[11]
(be) Department of Defense Foreign Clearance Manual, September 5, 2011[12]
(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, 2007[13]
(bm) Sections 102, 105, 552[14] and 552a[15] 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, 1991[16]
(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 2006[16]
(bu) Committee on National Security Systems Instruction 1001, "National Instruction on Classified Information Spillage," February 2008[16]
(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)

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 (l) 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 ~~12~~*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 (OUSD(P)).

(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 contactors 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.

l. 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 verses 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 (l).

(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 (l).

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 THE UNITED KINGDOM WITHOUT AN EXPORT LICENSE OR OTHER WRITTEN AUTHORIZATION

a. Background. 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, provides a comprehensive framework for exports and transfers of certain classified and unclassified defense articles, without an export license or other written authorization, to United Kingdom Communities (see Glossary). The provisions of the treaty 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 UK combined military or counter-terrorism operations;

(2) United States and UK cooperative security and defense research, development, production, and support programs;

(3) Mutually agreed specific security and defense projects where the Government of the United Kingdom is the end-user; or

(4) U.S. Government end-use.

c. Markings. Prior to transfer to the UK, defense articles that fall under the scope of the treaty 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 the

Defense Trade Cooperation Treaty between the United States and the UK and its Implementing Arrangement and must be used as specified.

(1) 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.

(2) Unclassified U.S. defense articles shall be marked:

//RESTRICTED USML//REL USA AND GBR TREATY COMMUNITY//

(3) 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.

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 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.

~~7~~*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 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.

~~8~~*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.

~~9~~*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 ~~9~~*10*.a.(1) of this section do not apply. Refer to section ~~10~~*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.

~~10~~*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 ~~9~~*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.

~~11~~*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 ~~9~~*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 ~~11~~*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).

~~12~~*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 ~~13~~*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.

~~13~~*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 ~~11~~*12* and ~~12~~*13*, paying particular attention to paragraph ~~11~~*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 ~~7~~*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.

GLOSSARY

PART 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
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.

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 content 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 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 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.