

**Army Regulation 380–5**

**Security**

# **Army Information Security Program**

**Headquarters  
Department of the Army  
Washington, DC  
25 March 2022**

**UNCLASSIFIED**

# ***SUMMARY of CHANGE***

AR 380–5

Army Information Security Program

This expedited revision, dated 25 March 2022—

- o Corrects the role of the Administrative Assistant to the Secretary of the Army as the Army program management official for the Offices of Headquarters, Department of the Army Principal Officials in the National Capital Region (para 1–6).
- o Adds corresponding reference for Secretary of the Army classification authority (paras 2–2*a* and 2–2*d*).
- o Adds a new paragraph on process for classification challenges (para 2–16).
- o Updates the website address for the information security policy team (para 2–19*c*(4)).
- o Omits obsolete references to “For Official Use Only” or “FOUO” terminology as prescribed by DoDI 5200.48 (chap 4 and throughout).
- o Removes references to DD Form 2056 (Telephone Monitoring Notification Decal), which was cancelled 10 December 2019 (para 5–12).
- o Adds definition of “legacy material” (glossary).
- o Replaces references to DoDM 5200.01, Volume 4, with DoDI 5200.48 addressing Controlled Unclassified Information (throughout).


Security  
**Army Information Security Program**

---

By Order of the Secretary of the Army:

**JAMES C. MCCONVILLE**  
General, United States Army  
Chief of Staff

Official:

  
**MARK F. AVERILL**  
Administrative Assistant to the  
Secretary of the Army

**History.** This publication is an expedited revision.

**Summary.** This regulation implements the policy set forth in Executive Order 13526; DoDM 5200.01, Volumes 1 through 3; and DoDI 5200.48.

**Applicability.** This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, the U.S. Army Reserve, and Department of the Army Civilian personnel, unless otherwise stated.

**Proponent and exception authority.**

The proponent of this regulation is the Deputy Chief of Staff, G–2. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The proponent may delegate this approval authority in writing to a division chief within the proponent agency in the grade of Colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific requirements.

**Army internal control process.**

This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see app B).

**Supplementation.** Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval by the Deputy Chief of Staff, G–2 (DAMI–CDS), [usarmy.pentagon.hqda-dcs-g-2.mbx.security-message@mail.mil](mailto:usarmy.pentagon.hqda-dcs-g-2.mbx.security-message@mail.mil).

**Suggested improvements.** Users of this regulation are invited to send comments and suggestions for improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G–2 (DAMI–CDS), [usarmy.pentagon.hqda-dcs-g-2.mbx.security-message@army.mil](mailto:usarmy.pentagon.hqda-dcs-g-2.mbx.security-message@army.mil).

**Distribution.** This regulation is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

---

**Contents** (Listed by paragraph and page number)

**Chapter 1**  
**General Provisions and Program Management, page 1**

*Section I*

*Introduction, page 1*

Purpose • 1–1, *page 1*

References and forms • 1–2, *page 1*

Explanation of abbreviations and terms • 1–3, *page 1*

Responsibilities • 1–4, *page 1*

Records management (recordkeeping) requirements • 1–5, *page 1*

*Section II*

*Responsibilities, page 1*

Administrative Assistant to the Secretary of the Army • 1–6, *page 1*

Deputy Chief of Staff, G–1 • 1–7, *page 1*

Deputy Chief of Staff, G–2 • 1–8, *page 1*

Commanders of Army commands, Army service component commands, and direct reporting units • 1–9, *page 2*

Commanders at all levels • 1–10, *page 2*

The security manager • 1–11, *page 3*

---

\*This regulation supersedes AR 380–5, dated 22 October 2019.

## **Contents—Continued**

Supervisors • 1–12, *page 4*  
All Army personnel • 1–13, *page 4*

### *Section III*

*Program Management, page 4*  
Applicability • 1–14, *page 4*  
General principles • 1–15, *page 4*

### *Section IV*

*Special Types of Information, page 5*  
Restricted Data and/or Formerly Restricted Data • 1–16, *page 5*  
Sensitive compartmented information, communications security information, and special access program information • 1–17, *page 5*

### *Section V*

*Exceptional Situations, page 6*  
Military operations, exercises, and unit deactivations • 1–18, *page 6*  
Waivers and exceptions to policy • 1–19, *page 6*

### *Section VI*

*Corrective Actions and Sanctions, page 6*  
General • 1–20, *page 6*  
Sanctions • 1–21, *page 7*  
Reporting of security incidents • 1–22, *page 7*

### *Section VII*

*Reports, page 7*  
Reporting requirements • 1–23, *page 7*  
Command security inspections • 1–24, *page 7*

## **Chapter 2**

### **Classification, page 7**

#### *Section I*

*Classification Principles, page 7*  
Original versus derivative classification • 2–1, *page 7*  
Delegation of authority • 2–2, *page 8*  
Required training • 2–3, *page 8*

#### *Section II*

*Derivative Classification, page 8*  
Policy • 2–4, *page 8*  
Accuracy responsibilities • 2–5, *page 8*  
Required training • 2–6, *page 9*

#### *Section III*

*The Original Classification Process, page 9*  
General • 2–7, *page 9*  
Classification criteria • 2–8, *page 9*  
Levels of classification • 2–9, *page 10*  
Duration of classification • 2–10, *page 10*  
Reclassification of information declassified and released to the public under proper authority • 2–11, *page 10*  
Communicating the classification decision • 2–12, *page 10*  
Compilation • 2–13, *page 10*  
Acquisition process • 2–14, *page 10*  
Limitations and prohibitions • 2–15, *page 11*  
Classification challenges • 2–16, *page 11*

## **Contents—Continued**

### *Section IV*

*Security Classification Guides, page 11*

Policy • 2–17, *page 11*

Content • 2–18, *page 11*

Approval, distribution, and indexing • 2–19, *page 11*

Review, revision, and cancellation • 2–20, *page 12*

### *Section V*

*Nongovernment Research and Development Information, page 13*

Policy • 2–21, *page 13*

## **Chapter 3**

**Declassification, Downgrading, Upgrading, and Destruction, *page 13***

### *Section I*

*Army Declassification Program, page 13*

General • 3–1, *page 13*

Special program manager • 3–2, *page 13*

Declassification of Restricted Data and Formerly Restricted Data • 3–3, *page 15*

Declassification of other than Army information • 3–4, *page 15*

### *Section II*

*The Automatic Declassification System, page 15*

General • 3–5, *page 15*

Exemption from automatic declassification • 3–6, *page 15*

Marking records exempted from automatic declassification • 3–7, *page 16*

Records review guidelines • 3–8, *page 17*

Army commands, Army service component commands, direct reporting units requirements • 3–9, *page 17*

### *Section III*

*Mandatory Declassification and Systematic Declassification Reviews, page 18*

Mandatory declassification reviews • 3–10, *page 18*

Mandatory declassification review appeals • 3–11, *page 18*

Systematic declassification reviews • 3–12, *page 18*

### *Section IV*

*Change in the Level of Classification, page 19*

General • 3–13, *page 19*

Downgrading • 3–14, *page 19*

Upgrading • 3–15, *page 19*

### *Section V*

*Classified Material Destruction Standards, page 19*

General • 3–16, *page 19*

Approved routine methods of destruction • 3–17, *page 19*

Technical advice on approved destruction devices and methods • 3–18, *page 20*

## **Chapter 4**

**Controlled Unclassified Information, *page 20***

General • 4–1, *page 20*

## **Chapter 5**

**Access, Control, Safeguarding, and Visits, *page 20***

### *Section I*

*Access, page 20*

Responsibilities • 5–1, *page 20*

## **Contents—Continued**

Nondisclosure agreement • 5–2, *page 20*  
Signing and filing the nondisclosure agreement • 5–3, *page 21*  
Refusal to execute the nondisclosure agreement • 5–4, *page 21*  
Debriefing and termination of classified access • 5–5, *page 21*  
Access to Restricted Data, Formerly Restricted Data, and critical nuclear weapon design information • 5–6, *page 22*  
Access by persons outside the Executive Branch • 5–7, *page 22*

### *Section II*

*Control Measures and Visits, page 23*  
Responsibilities • 5–8, *page 23*  
Care during working hours • 5–9, *page 23*  
End-of-day security checks • 5–10, *page 24*  
Emergency planning • 5–11, *page 24*  
Classified discussions • 5–12, *page 25*  
Removal of classified storage and information technology equipment • 5–13, *page 25*  
Visits • 5–14, *page 25*  
Classified meetings and conferences • 5–15, *page 25*

### *Section III*

*Accountability and Administrative Procedures, page 27*  
Equipment used in information technology networks • 5–16, *page 27*  
Receipt of classified material • 5–17, *page 27*  
Top Secret information • 5–18, *page 27*  
Foreign government information • 5–19, *page 28*  
Working papers • 5–20, *page 29*  
Reproduction of Classified Material • 5–21, *page 29*

### *Section IV*

*Disposition and Destruction of Classified Material, page 30*  
Policy • 5–22, *page 30*  
Methods and standards for destruction • 5–23, *page 30*  
Records of destruction • 5–24, *page 31*

## **Chapter 6**

### **Storage and Physical Security Standards, page 31**

#### *Section I*

*General, page 31*  
Policy • 6–1, *page 31*  
Physical security policy • 6–2, *page 31*

#### *Section II*

*Storage Standards, page 31*  
Standards for storage equipment • 6–3, *page 31*  
Storage of classified information • 6–4, *page 31*  
Procurement of new storage equipment • 6–5, *page 33*  
Removal of classified information for work at home • 6–6, *page 33*  
Safeguarding of U.S. classified information located in foreign countries • 6–7, *page 33*  
Equipment designations and combinations • 6–8, *page 34*  
Neutralization and repair of Government Services Agency-approved security containers and vault doors • 6–9, *page 34*  
Maintenance and operating inspections • 6–10, *page 35*  
Turn-in or transfer of security equipment • 6–11, *page 35*

#### *Section III*

*Physical Security Standards, page 35*  
General • 6–12, *page 35*

## **Contents—Continued**

Vault and secure room (open storage area) construction standards • 6–13, *page 35*  
Intrusion detection system standards • 6–14, *page 36*  
Selection of equipment • 6–15, *page 37*  
Intrusion detection system transmission and annunciation • 6–16, *page 37*  
System requirements • 6–17, *page 38*  
Installation, maintenance, and monitoring • 6–18, *page 38*  
Access controls while material is not secured in security containers • 6–19, *page 38*

### **Chapter 7**

#### **Transmission and Transportation, *page 40***

##### *Section I*

*Methods of Transmission or Transportation, page 40*

Policy • 7–1, *page 40*

Dissemination outside the Department of Defense • 7–2, *page 40*

Top Secret information • 7–3, *page 41*

Secret information • 7–4, *page 41*

Confidential information • 7–5, *page 42*

##### *Section II*

*Transmission and Transportation of Classified Material, page 42*

Transmission and transportation of classified material to foreign governments • 7–6, *page 42*

Preparation of material for shipment by freight • 7–7, *page 43*

Envelopes or containers • 7–8, *page 43*

Addressing • 7–9, *page 43*

Mail channels with other government agencies • 7–10, *page 44*

##### *Section III*

*Escort or Hand-Carrying of Classified Material, page 44*

General provisions • 7–11, *page 44*

Documentation • 7–12, *page 44*

Hand-carrying or escorting classified material aboard commercial passenger aircraft • 7–13, *page 45*

Consignor/consignee responsibility for shipment of bulky material • 7–14, *page 46*

### **Chapter 8**

#### **Security Education and Training, *page 46***

##### *Section I*

*Policy, page 46*

General policy • 8–1, *page 46*

Methodology • 8–2, *page 47*

##### *Section II*

*Briefings and Training, page 47*

Initial security orientation • 8–3, *page 47*

Annual refresher training • 8–4, *page 47*

Training for managers and supervisors • 8–5, *page 48*

##### *Section III*

*Special Requirements, page 48*

General policy • 8–6, *page 48*

Original classifiers • 8–7, *page 48*

Derivative classifiers • 8–8, *page 48*

Security program management personnel • 8–9, *page 48*

North Atlantic Treaty Organization briefing for cleared personnel • 8–10, *page 49*

Others • 8–11, *page 49*

Termination briefings • 8–12, *page 49*

## **Contents—Continued**

Program management • 8–13, *page 50*

### **Chapter 9**

#### **Security Incidents and Reporting Involving Classified Information, *page 50***

##### *Section I*

##### *Policy, page 50*

Terms and categories of security incidents • 9–1, *page 50*

Reporting and notifications • 9–2, *page 51*

Security inquiries and investigations • 9–3, *page 51*

Classified information appearing in the public media • 9–4, *page 52*

Reporting results of the inquiry • 9–5, *page 52*

Reevaluation and damage assessment • 9–6, *page 52*

Debriefings in cases of unauthorized access • 9–7, *page 52*

Management and oversight • 9–8, *page 53*

Unauthorized absences, suicides, or incapacitation • 9–9, *page 53*

Negligence • 9–10, *page 54*

### **Appendixes**

**A.** References, *page 55*

**B.** Internal Control Evaluation, *page 61*

### **Figure List**

Figure 3–1: Sample letter of certification, *page 14*

### **Glossary**



## **Chapter 1**

### **General Provisions and Program Management**

#### **Section I**

##### **Introduction**

###### **1–1. Purpose**

This regulation develops Department of the Army (DA) policy for the classification, downgrading, declassification, transmission, transportation, and safeguarding of information requiring protection in the interests of national security. It primarily pertains to classified national security information, or classified information, but also addresses Controlled Unclassified Information (CUI). For purposes of this regulation, classified national security information, or classified information, is defined as information and/or material that has been determined, pursuant to Executive Order (EO) 13526, or any applicable predecessor order, to require protection against unauthorized disclosure and is marked to indicate its appropriate classification. This regulation implements EO 13526; EO 13556; DoDM 5200.01, Volumes 1 through 3; and DoDI 5200.48. This regulation also establishes policy on the safeguards of Restricted Data (RD) and Formerly Restricted Data (FRD), as specified by the Atomic Energy Act of 1954, as amended.

###### **1–2. References and forms**

See appendix A.

###### **1–3. Explanation of abbreviations and terms**

See glossary.

###### **1–4. Responsibilities**

Responsibilities are listed in section II of this chapter.

###### **1–5. Records management (recordkeeping) requirements**

The records management requirement for all record numbers, associated forms, and reports required by this publication are addressed in the Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at <https://www.arims.army.mil>. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

#### **Section II**

##### **Responsibilities**

###### **1–6. Administrative Assistant to the Secretary of the Army**

The AASA is designated the Army program management official responsible for ensuring implementation of the information security program for Headquarters, Department of the Army (HQDA)/Operating Agency–22 (OA–22) organizations in the National Capital Region.

###### **1–7. Deputy Chief of Staff, G–1**

The DCS, G–1 is responsible for executing the provisions of EO 13526, Section 5.4(d)(7), and will ensure that the systems used to evaluate or rate civilian and military personnel performance include management of classified information as a critical element or item to be evaluated in the rating of:

- a. Original classification authorities.
- b. Security managers (SMs) or security specialists.
- c. All other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings.

###### **1–8. Deputy Chief of Staff, G–2**

The DCS, G–2, will act as the designated DA senior agency official by the Secretary of the Army (SECARMY), to direct, administer, and oversee the Army's information security program. The DCS, G–2, will—

- a. Develop, coordinate, and oversee the Army Information Security Program.

- b.* Provide program management through issuance of policy and operating guidance.
- c.* Ensure DA commands adequately resource the program and meet established policies and procedures.
- d.* Ensure all DA commands integrate security education, training, and awareness into their information security programs pursuant to EO 13526, DoDM 5200.01, Volume 3 and DoDI 5200.48.
- e.* Provide staff assistance to DA commands in resolving day-to-day security policy and operating problems.
- f.* Formulate policy governing the submission of security incident reports.
- g.* As a Top Secret original classification authority (OCA), delegate Secret and Confidential OCA to other Army officials where appropriate.
- h.* The Director, Counterintelligence, Human Intelligence, Security and Disclosure (DAMI-CD), on behalf of the DCS, G-2, manages and provides oversight of all aspects of the Army Information Security Program. The Director (DAMI-CD) will—
  - (1) Maintain a centralized system of control and coordination of security incident reporting and any resulting information security investigations worldwide.
  - (2) Ensure that policy, procedures, and programs are developed for the implementation of EO 13526, EO 13556, DoDM 5200.01, Volumes 1 through 3, DoDI 5200.48, and other DoD issuances that implement EO 13526 and EO 13556.
  - (3) Monitor, evaluate, and report on the administration of the Army's information security program. Ensure that Army commands (ACOMs), Army service component commands (ASCCs), and direct reporting units (DRUs) establish and maintain an ongoing self-inspection program, which includes periodic reviews and assessments of their classified and CUI.
  - (4) Respond to information security matters pertaining to classified information that originated in an ACOM that no longer exists and for which there is no successor in function.
  - (5) Commit the resources required for the effective development of policy and oversight of the programs established by this regulation.
  - (6) Serve as the approving authority of an information security curriculum for an Army Security Education, Training, and Awareness Program.

#### **1-9. Commanders of Army commands, Army service component commands, and direct reporting units**

Commanders of ACOMs, ASCCs, and DRUs will—

- a.* Establish an information security program and ensure that all DA personnel execute procedures and processes in accordance with this regulation and related DoD issuances.
- b.* Ensure an SM is appointed in writing for the command and subordinate commands, activities, and agencies that create, handle, or store classified information and CUI to oversee the command's information security program. The SM should be of sufficient rank or grade to effectively discharge assigned duties and responsibilities. As a general requirement, the SM will be a commissioned officer (O - 3 or above), warrant officer, or civilian in the grade of GS - 11/12 or above (or pay band equivalent).
- c.* Ensure all SMs are afforded security training consistent with assigned duties and this regulation.
- d.* Review and inspect the effectiveness of the information security program within the command annually or more frequently based on program needs and the degree of involvement with managing classified information.
- e.* Provide oversight of the responsibilities listed in paragraph 1-8 for subordinate commands.
- f.* Ensure that all incidents specified in this regulation are reported accordingly.
- g.* Include the management of classified information as a critical element or item in personnel performance evaluations, where appropriate as directed in the provisions of EO 13526.

#### **1-10. Commanders at all levels**

Commanders at all levels and heads of agencies and activities are responsible for effective management of the information security program within commands, agencies, activities, or areas of responsibility (referred to within this regulation as commands). Commanders may delegate certain authorities to execute the requirements of this regulation, where applicable, but not their program management responsibilities. Security, including the safeguarding of classified and CUI and the appropriate classification and declassification of information created by DA personnel, is the responsibility of the commander. The commander will—

- a.* Establish written local information security policies and procedures and an effective information security education program, consistent with this regulation.
- b.* Formulate and supervise measures or instructions necessary to ensure continuous protection of classified information, CUI, and related materials.

- c. Ensure that persons requiring access to classified information have met the appropriate security clearance eligibility, access standards, and have a need-to-know.
- d. Continually assess the individual trustworthiness of personnel who possess security clearance eligibility and who have been given access to classified information.
- e. Designate an SM in writing. Ensure the SM is of sufficient rank or grade to effectively discharge assigned duties and responsibilities.
- f. Ensure the SM has been the subject of a favorably adjudicated, current background investigation appropriate for the highest level of classification of information and the appropriate access to the level of information managed.
- g. Ensure the SM receives security training consistent with assigned duties and this regulation.
- h. Ensure adequate funding and personnel are available to allow security management personnel to manage and administer applicable information security program requirements.
- i. Review and inspect the effectiveness of the information security program within the command annually or more frequently based on program needs and classification activity.
- j. Ensure prompt and appropriate responses are given, or forwarded for higher echelon decision, to any problems, suggestions, requests, appeals, challenges, or complaints arising out of the implementation of this regulation.
- k. Ensure the prompt and complete reporting of security incidents, violations, and compromises related to classified information or the unauthorized disclosure of CUI, as directed herein and DoDI 5200.48.
- l. Ensure violations of this regulation, including suspected compromises or other threats to the safeguarding of classified information and the unauthorized disclosure of CUI, are reported and investigated in accordance with this regulation.
- m. Ensure prompt reporting of credible derogatory information on assigned or attached personnel and contractors, to include recommendations for or against continued access to classified information in accordance with AR 380–49 and AR 380–67.
- n. Ensure compliance with the requirements of this regulation when access to classified information is provided to industry at a facility or location for which the command is responsible, in connection with a classified contract. If the classified information is provided to industry at the contractor’s facility, ensure compliance with the provisions of AR 380–49.
- o. Include the management of classified information as a critical element or item in personnel performance evaluations where appropriate, as directed in the provisions of EO 13526.

## **1–11. The security manager**

The SM is the principal advisor on information security in the command, and is responsible to the commander for management of the program. The SM will have direct access to the commander on matters affecting the information security program. The SM will—

- a. Advise and represent the commander on matters related to the classification, downgrading, declassification, and safeguarding of national security information.
- b. Establish and implement an effective security education program for the command as required by chapter 8 of this regulation.
- c. Establish procedures for ensuring that DA personnel who handle classified material are properly cleared in accordance with AR 380–67.
- d. Advise and assist officials on classification problems and the development of classification guidance.
- e. Ensure that classification guides for classified plans, programs, projects, or mission are properly prepared, approved, distributed, and maintained.
- f. Conduct a periodic review of classifications assigned within the activity, to ensure classification decisions are consistent with DoD classification guidelines.
- g. Consistent with operational and statutory requirements, review classified and CUI documents in coordination with the command records management officer. Continually reduce, by declassification, destruction, decontrol, or retirement, as appropriate, unneeded classified information and CUI.
- h. Oversee or conduct security inspections and spot checks for compliance with this regulation and other security regulations and directives, and notify the commander of the results.
- i. Assist and advise the commander in matters pertaining to the enforcement of regulations governing the access to, and the dissemination, reproduction, transmission, transportation, safeguarding, and destruction of classified information or CUI and material.
- j. Make recommendations, based on applicable regulations and directives, on requests for visits by foreign nationals and foreign government representatives. Provide security and disclosure guidance if the visit request is approved. For further guidance regarding official visits by foreign government representatives, refer to AR 380–10.

*k.* Ensure violations of this regulation, including suspected compromises or other threats to the safeguarding of classified information and the unauthorized disclosure of CUI, are reported and investigated in accordance with this regulation. Recommend appropriate corrective actions to address security violations.

*l.* Ensure proposed public releases concerning classified or sensitive programs are reviewed to preclude the release of classified information, CUI, or other sensitive unclassified information exempt from release under the Freedom of Information Act (FOIA).

*m.* Establish and maintain visitor control procedures in cases in which visitors are authorized access to classified information or to areas where classified material is stored and or processed.

*n.* Issue contingency plans for the emergency destruction of classified information, when necessary, and for the safeguarding of classified information used in or near hostile or potentially hostile areas.

*o.* Be the single point of contact to coordinate and resolve classification or declassification problems.

*p.* Report data as required by this regulation.

## **1–12. Supervisors**

Supervisory personnel have a key role in the effective implementation of the command's information security program. Supervisors, by example, words, and deeds, set the tone for compliance by subordinate personnel with the requirements to properly safeguard, classify, and declassify information related to national security. Supervisors will—

*a.* Ensure subordinate personnel who require access to classified information are properly cleared in accordance with AR 380–67.

*b.* Ensure subordinate personnel are trained in, and comply with the requirements of this regulation, as well as local policy and procedures concerning the information security program.

*c.* Continually assess the eligibility of subordinate personnel for access to classified information, and report to the SM any information that may have a bearing on that eligibility in accordance with AR 380–67.

*d.* Include the management of classified information as a critical element or item in personnel performance evaluations, where appropriate.

## **1–13. All Army personnel**

All DA personnel, regardless of rank, title, or position, have a personal, individual, and official responsibility to safeguard information related to national security they have access to. All DA personnel will report, to the proper authority, actions by others or any other matters that could lead to, or that have resulted in, the unauthorized disclosure or compromise of classified information or CUI.

## **Section III**

### **Program Management**

#### **1–14. Applicability**

This regulation governs the DA information security program and applies to all DA personnel as defined in the terms section of the glossary. Contractors will comply with the terms of this regulation and any information security program requirements as required by the terms of their contracts.

#### **1–15. General principles**

*a.* DA personnel and DA contractors will mark all classified information and material, regardless of media (for example, paper documents, emails, slide presentations, and web pages) in accordance with DoDM 5200.01, Volume 2. CUI will be marked in accordance with DoDI 5200.48.

(1) In the event of any marking conflict with this regulation, DoDM 5200.01, Volume 2, DoDI 5200.48 or other Army regulations, personnel will follow the DoDM 5200.01, Volume 2 and DoDI 5200.48.

(2) Where DoDM 5200.01, Volume 1 refers to waivers and/or exceptions, all requests will be through DCS, G–2 (DAMI–CD) and in accordance with paragraph 1–19.

*b.* This regulation does not establish policy for the safeguarding of special category information which is covered elsewhere, to include AR 380–28, AR 380–40, special access programs (SAPs), and alternative compensatory control measures (see AR 380–381).

*c.* Information may be originally classified only if all of the following conditions are met:

(1) An OCA is classifying the information.

(2) The information is owned by, produced by or for, or is under the control of the U.S. Government.

- (3) The information falls within one or more of the classification categories listed in EO 13526, Section 1.4.
- (4) The OCA determines the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the anticipated damage.
- d. If there is significant doubt about the need to classify information, it will not be classified. This provision does not:
  - (1) Amplify or modify the substantive criteria or procedures for classification; or
  - (2) Create any substantive or procedural rights subject to judicial review.
- e. Classified information will not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.
- f. The unauthorized disclosure of foreign government information (FGI) is presumed to cause damage to the national security.
- g. Information or material that requires protection against unauthorized disclosure in the interest of national security, will be classified as one of the three following categories or levels, as defined in EO 13526:
  - (1) Top Secret.
  - (2) Secret.
  - (3) Confidential.
- h. Except as otherwise provided by statute, no other terms will be used to identify U.S. classified information. If there is significant doubt about the appropriate level of classification, it will be classified at the lower level.
- i. Information and material will be afforded the level of protection against unauthorized disclosure commensurate with the level of classification or controls assigned, under the varying conditions that may arise in connection with its use, dissemination, storage, movement, transmission, or destruction. All DA personnel will ensure classified information and CUI are adequately protected from compromise and must be continually aware of possible threats from all-source intelligence efforts of potential adversaries.
- j. Access to classified information is authorized only to personnel:
  - (1) With the appropriate need-to-know the information in order to perform a lawful and authorized governmental function;
  - (2) Who have been granted security clearance eligibility and access at the appropriate level (see AR 380–67); and
  - (3) Who have executed an appropriate nondisclosure agreement (NDA).
- k. The holder of the information, not the potential recipient, determines the need-to-know and is responsible for verifying the clearance and access of the potential recipient. No person will be granted access to classified information solely by virtue of grade, rank, title, or position.
- l. Classified information and CUI will be maintained in the organization only when necessary for the operation of the organization or when its retention is required by law, regulation, or records management policy.

## **Section IV**

### **Special Types of Information**

#### **1–16. Restricted Data and/or Formerly Restricted Data**

EO 13526 does not apply to information classified as RD or FRD. RD and FRD will not be declassified without the specific permission of the U.S. Department of Energy (DOE). Policy on the marking of RD or FRD is contained in DoDM 5200.01, Volume 2. RD and FRD will be safeguarded as required by this regulation and DoD directives referenced herein. The policy on the classification, downgrading, and declassification of RD and FRD is stated in classification and declassification guidance promulgated by the DOE, or in guidance issued jointly by the DoD and DOE.

#### **1–17. Sensitive compartmented information, communications security information, and special access program information**

Security classification and declassification policies apply to sensitive compartmented information (SCI), communications security (COMSEC), and SAP information in the same manner as other classified information (See DoDM 5200.01, Volume 1 for declassification of cryptologic information). SCI, COMSEC, and SAP information will be controlled and safeguarded in accordance with AR 380–28, AR 380–40, and AR 380–381, respectively.

## Section V

### Exceptional Situations

#### 1–18. Military operations, exercises, and unit deactivations

*a. Military operations.* Commanders may modify, but not lessen, standards pertaining to accountability, dissemination, transmission, and storage of classified information, as necessary, to meet local conditions encountered during military operations. Military operations include combat operations, emergency conditions under operations other than war (to include peacekeeping operations), and any other emergency situation where that operation or situation requires exceptional measures to protect life or DA assets. Classified information will be introduced into combat areas or zones, or areas of potential hostile activity, only as necessary to accomplish the military mission.

*b. Military exercises.* Military exercises pose a unique situation when handling and protecting classified information or material. Documents and material that contain no classified information, but which carry classification markings for training purposes or to provide an example, will also have a marking that clearly shows the actual classification (or dissemination control marking) of the documents. (See DoDM 5200.01, Volume 2 for marking of this type). When real-world classified and/or CUI is introduced or used in military exercises, every effort will be taken to prevent compromise and/or loss.

*c. Unit deactivation.* OCA is assigned to a duty position, not to an individual person. When an organization has been deactivated, the OCA's responsibilities will revert to the higher headquarters or to the organization assuming responsibility for the deactivated organization's security decisions. Challenges to classification decisions of the deactivated organization will be directed to the headquarters element that assumes the security responsibilities of the deactivated unit.

#### 1–19. Waivers and exceptions to policy

*a.* Unless otherwise specified herein, requests for waivers or exceptions to the provisions in this regulation will be submitted, through command channels, to DCS, G–2 (DAMI–CD). Waivers and exceptions to DoD requirements will be forwarded by DCS, G–2 (DAMI–CD) for decision to the appropriate DoD agency in accordance with DoDM 5200.01, Volumes 1 through 3.

*b.* Requests for waivers will contain sufficient information to permit a complete and thorough analysis to be made of the impact of approval on national security. At a minimum, requests must identify the specific provision(s) of this regulation or other authority for which the waiver or exception is sought and provide a rationale and justification for the request.

*c.* The request must describe the mission need and any associated risk management considerations (for example, negative impact to cost, schedule, mission, or operations) or provisions, including a summary of proposed mitigation measures to reduce risk, and the timeframe (the proposed duration if requesting a waiver, and permanent if requesting an exception). (See glossary for definitions of waiver and exception.)

*d.* The requestor will maintain documentation regarding all approved waivers and exceptions, and furnish this documentation, upon request, to other agencies and to other DA commands with which classified information or secure facilities are shared.

*e.* Waivers or exceptions granted before the effective date of this regulation are canceled no later than 1 year after the effective date of this regulation. New and updated requests may be submitted prior to the cancellation date.

*f.* Throughout this regulation, there are references to policy subject to ACOM, ASCC, and DRU approval or subject to policy as the ACOM, ASCC, and DRU may direct. Where that language, in substance, is used, the commanders of ACOMs, ASCCs, DRUs, and the AASA, may delegate approval authority to a subordinate element within the command. The commander or the AASA will maintain a written copy of the delegation and review it periodically. Where this regulation specifically grants waiver or exception authority to an ACOM, ASCC, or DRU level commander or the AASA, that authority resides solely with the ACOM, ASCC, or DRU commander or AASA and will not be further delegated.

## Section VI

### Corrective Actions and Sanctions

#### 1–20. General

Commanders will establish procedures to ensure that prompt and appropriate action is taken in cases of compromise of classified information or unauthorized disclosure of CUI; improper classification or designation of information; violations of the provisions of this regulation; and incidents that may put classified information and CUI at risk of

unauthorized disclosure. Such actions will focus on correction or elimination of the conditions that caused or contributed to the incident.

### **1–21. Sanctions**

- a.* DA personnel will be subject to sanctions if they knowingly, willfully, or negligently—
  - (1) Disclose classified information or CUI to persons not authorized to receive it;
  - (2) Classify or continue the classification of information in violation of this regulation; or
  - (3) Violate any other provision of this regulation.
- b.* Sanctions can include, but are not limited to warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information and/or CUI, and removal of classification authority. Action can also be taken under the Uniform Code of Military Justice for military personnel, if warranted.
- c.* OCA will be withdrawn from individuals who demonstrate a disregard or pattern of error in applying the classification standards of this regulation.
- d.* DoDM 5200.01, Volume 3, Enclosure 6 addresses sanctions against contractor personnel. Disciplinary action and sanctions are the responsibility of the contractor's company unless specific contract provisions address such actions.

### **1–22. Reporting of security incidents**

EO 13526, Section 5.5, requires that the Director of the Information Security Oversight Office (ISOO) be advised of instances in which properly classified information is knowingly, willfully, or negligently disclosed to unauthorized persons; instances of classifying or continuing the classification of information in violation of EO 13526 or any implementing directive, including this regulation; or creating or continuing an SAP contrary to EO 13526. Reports of security incidents will be submitted through command channels to the DCS, G–2 (DAMI–CD), for forwarding to the Director of the ISOO. See chapter 9 for reporting of security incidents.

## **Section VII**

### **Reports**

### **1–23. Reporting requirements**

HQDA must report data necessary to support various requirements of EO 13526. Commanders of ACOMs, ASCCs, DRUs, and the AASA will also submit a consolidated annual report for all units under their security responsibility on standard form (SF) 311 (Agency Security Classification Management Program Data) or other generated DoD reporting form to DCS, G–2 (DAMI–CD), no later than 1 October or other date specified by DCS, G–2 (DAMI–CD), each year. The report will cover the preceding fiscal year. DCS, G–2 (DAMI–CD) will consolidate and submit the annual SF 311 report for the DA.

### **1–24. Command security inspections**

Commanders of ACOMs, ASCCs, DRUs, and the AASA will establish and maintain a self-inspection program for their command, and a program to inspect their subordinate units. Self-inspections will be conducted annually or more frequently based on program needs and the degree of involvement with managing classified information. The purpose of the program will be to evaluate the effectiveness of the command's protection of classified and CUI, and adherence to policy contained in this regulation and DoD directives. The test questions located in appendix B may serve as the basis for the annual inspection and can incorporate additional questions as determined by the agency or command performing the inspection.

## **Chapter 2 Classification**

### **Section I**

### **Classification Principles**

### **2–1. Original versus derivative classification**

- a.* Original classification decisions can only be made by persons designated in writing by the SECARMY or the DCS, G–2. There are a limited number of officials in the Army that have the authority to apply original classification, and very limited instances of original classification.

*b.* Original classification is the initial determination that information requires, in the interests of national security, protection against unauthorized disclosure. This decision will be made only by persons specifically authorized in writing to do so and who have received training. The decision to originally classify must be made based on the requirements of this regulation. Delegations of OCA will be limited to the minimum required and only to officials who have a demonstrable and continuing need to exercise it.

*c.* Derivative classification is incorporating, restating, paraphrasing, or generating in new form, information that has already been determined to be classified and ensuring it is classified and handled at the level the OCA has already determined. Derivative classification is most commonly accomplished by marking classified material based on the guidance from a security classification guide (SCG) or from the source document. The derivative classifier must have enough subject matter knowledge to properly interpret and apply the instruction of the classification guidance. The OCA decides what portion(s) of a plan, program, project, or mission need to be classified. The derivative classifier applies that decision to the same type of information restated or generated in a new form.

## **2-2. Delegation of authority**

*a.* Top Secret OCA can be delegated only by the SECARMY in accordance with EO 13526 and Volume 75, Federal Register, p. 735–736 (referenced in app A). Secret and Confidential OCA can only be delegated by the DCS, G–2 (senior agency official) or by the SECARMY in accordance with EO 13526 and DoDM 5200.01, Volume 1. Delegation of classification authority includes authority to classify information at that level and any lower level(s) of classification. This authority cannot be further delegated.

*b.* Requests for OCA will be submitted through command channels to the DCS, G–2 (DAMI–CD). These requests will specify the position title for which the authority is requested and detailed justification for the request. OCA is assigned to a position, not to an individual person. To ensure that the number of OCAs is strictly limited, the request must address why another OCA within that official’s command cannot assume this responsibility.

*c.* Requests for OCA will be granted only when:

- (1) Original classification is required during the normal course of operations;
- (2) Sufficient expertise and information is available to the prospective OCA to ensure effective classification decision making; and
- (3) The need for original classification cannot be handled by other existing OCAs and referral of decisions to existing original classification authorities, at the command or at higher levels in the chain of command, is not practical.

*d.* Delegation of OCA by either the SECARMY or the DCS, G–2, may only be exercised to classify information relating to activities conducted under Army authorities. Officials occupying positions that have been delegated OCA by the SECARMY or DCS, G–2, may not use this authority while assigned, attached, or detailed to a combatant command to originally classify activities conducted under the command and control of a combatant commander (see DoDM 5200.01, Volume 1).

## **2-3. Required training**

Officials who have been delegated OCA will receive training as required by chapter 8 of this regulation and before exercising this authority. OCAs will certify in writing that they have received this training. Training will be completed on an annual basis thereafter.

## **Section II**

### **Derivative Classification**

## **2-4. Policy**

Derivative classification can be completed by any properly cleared and trained personnel. No appointment or designation is necessary unless directed by commanders of an ACOM, ASCC, or DRU or AASA.

## **2-5. Accuracy responsibilities**

Persons who sign or approve derivatively classified material are responsible for the accuracy of the derivative classification. This applies to all forms of material and information regardless of the media involved. Personnel accomplishing derivative classification will—

*a.* Observe and respect the classification determinations made by original classification authorities.

*b.* Apply markings or other means of identification to the derivatively classified material, in accordance with DoDM 5200.01, Volume 2, at the level and for the duration specified by the classification guide or source document. Where classification instructions do not reflect the new marking requirements of EO 13526, the level of classification



will be marked as directed by the SCG or source document and DoDM 5200.01, Volume 2, will be followed for all other marking requirements. Derivative classifiers are encouraged to keep records of which portions of a draft document are classified and by which source to make the classification of the finished product easier.

c. Only authorized sources such as classification guides, other forms of official classification guidance, and markings on source material from which the information is extracted will be used.

d. Use caution when paraphrasing or restating information extracted from a classified source to determine whether the classification could have been changed in the process.

e. Take appropriate and reasonable steps to resolve doubt or conflicts in classification. In cases of apparent conflict between an SCG and a classified source document concerning a discrete item of information, the instructions in the SCG will take precedence unless the source document is signed by the OCA. In such cases, the OCA, or the point of contact for answering questions on classification, will be consulted. If it is not possible to consult with the OCA, the more restrictive classification instruction will be followed.

f. Make a list of sources used when material is derivatively classified based on “Multiple Sources” (more than one SCG, classified source document, or any combination). A copy of this list will be included in, or attached to, the file or record copy of the material. Derivative classifiers are encouraged to include this listing with all copies of the document, to make later declassification review easier if the file or record copy is unavailable.

g. Contact the classifier of the source document for resolution in cases in which the derivative classifier believes the classification applied to the information is not accurate.

## **2-6. Required training**

DA personnel will receive training before derivatively classifying information, as required by chapter 8 of this regulation. Derivative classification training must be completed yearly thereafter.

## **Section III**

### **The Original Classification Process**

#### **2-7. General**

The decision to apply original classification requires the application of judgment on the part of the classifier that the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security, and that the probable damage can be identified or described. It is not necessary for the original classifier to produce a written description of the damage at the time of classification, but the classifier must be prepared to do so if the information becomes the subject of a classification challenge, a request for mandatory review for declassification, or a request for release under FOIA. The decision to classify also has operational and resource impacts as well as impacts affecting the United States technological base and foreign relations. The decision to classify should consider all relevant factors. If there is doubt about classification, the OCA will research the matter to make an informed decision. If, after such research, there is a significant doubt about the need to classify information, it will not be classified. Additional policies and procedures about OCA are found in DoDM 5200.01, Volume 1.

#### **2-8. Classification criteria**

U.S. classification can only be applied to information that is owned by, produced by or for, or is under the control of, the U.S. Government. The OCA determines whether the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the information falls within one or more of the following categories specified in EO 13526:

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

## **2-9. Levels of classification**

*a.* Once a decision is made to classify, information will be classified at one of the three levels listed below. For each level, the OCA must be able to identify or describe the damage that unauthorized disclosure reasonably could be expected to cause to the national security. These levels are as follows:

(1) *Top Secret.* Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

(2) *Secret.* Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

(3) *Confidential.* Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause damage to the national security.

*b.* If there is doubt about the classification level, the OCA will research the matter to make an informed decision. If significant doubt remains about the classification level to be assigned, the lower level will be assigned.

## **2-10. Duration of classification**

Information will be declassified as soon as it no longer meets the standards for classification. Information will remain classified if it is in the interest of national security and meets the criteria of EO 13526. At the time an item of information is originally classified, the original classifier must decide the length of time the information will require classification and select an appropriate declassification date or event for declassification based on the duration of the national security sensitivity of the information. Additional policies and procedures regarding the duration of classification are found in DoDM 5200.01, Volume 1.

## **2-11. Reclassification of information declassified and released to the public under proper authority**

*a.* The OCA must determine that, if classification is applied or reapplied, there is a reasonable possibility the information will be provided protection from unauthorized disclosure.

*b.* Reclassification is accomplished on a document-by-document basis, with the participation, or under the direction of, the SECARMY, the Under SECARMY, or the DCS G-2. Guidance from DCS, G-2 (DAMI-CD) will be requested in these instances. The information that is reclassified must meet the criteria for classified information established in EO 13526 or successor orders and directives. Additional policies and procedures regarding reclassification are found in DoDM 5200.01, Volume 1.

## **2-12. Communicating the classification decision**

An OCA who has decided to originally classify information is responsible for communicating that decision to persons who will likely be in possession of that information. This will be accomplished by issuing classification guidance, discussed in section V of this chapter, or by ensuring that documents containing the information are properly marked to reflect the decision.

*a.* In rare situations where the OCA's decision must be rendered verbally due to priorities of an ongoing operation, written confirmation will be issued within 7 calendar days of the decision and provide the required declassification and marking instructions.

*b.* Decisions made and issued by other than a classification or declassification guide (for example, in the form of a memorandum, plan, or order) should be incorporated in an SCG as soon as possible.

## **2-13. Compilation**

In unusual circumstances, compilation of items of information that are individually unclassified can be classified if the compiled information reveals an additional association or relationship that matches criteria for classification as described in paragraph 2-8 of this regulation. Classification by compilation will be fully supported by a written explanation that will be provided on, in, or with the material containing the information. Any classification as a result of compilation requires an original classification decision by an OCA. Additional policies and procedures regarding classification by compilation are found in DoDM 5200.01, Volume 1.

## **2-14. Acquisition process**

Classification and safeguarding of information involved in the DoD acquisition process will conform to the standards of this regulation, as well as the requirements of DoDD 5000.01 and DoDI 5000.02 (or successor directives and instructions). SCGs should be updated to include classified critical program information (CPI) identified as part of the program protection planning process required by DoDI 5200.39.

## **2–15. Limitations and prohibitions**

EO 13526 and the Atomic Energy Act of 1954, as amended (Section 2011, Title 42, United States Code (42 USC 2011 et seq.)), provide the only basis to classify information. Classification cannot be used to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization, agency, or to restrain competition. Basic scientific research and its results can be classified only if it clearly relates to the national security. Section V of this chapter covers information that is a product of nongovernment research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access.

## **2–16. Classification challenges**

a. If holders of information have substantial reason to believe information is improperly or unnecessarily classified, they will communicate that belief through their SM to the OCA of the information. This may be done informally or by submitting a formal challenge to the classification as provided for in EO 13526. Informal questioning of classification is encouraged before resorting to a formal challenge.

(1) Commanders will establish written procedures through which holders of classified information within their commands can challenge a classification decision and will ensure that command personnel are made aware of the established procedures. Commanders will make sure that no retribution is taken against any personnel for making a challenge to a classification.

(2) Formal challenges to classification will include a sufficient description of the information being challenged to permit identification of the information and its classifier, to include the OCA, where known, with reasonable effort. Challenges to classification made by DA personnel will include the reason why the challenger believes that the information is improperly or unnecessarily classified. The challenge request should be unclassified, if possible.

(3) Pending a final decision of any challenge the classification of the information being challenged will be upheld and carried forward until otherwise determined by the appropriate authorized official.

b. The following will be established by each OCA:

(1) Written procedures through which holders of classified information within or outside of their command can challenge classification decisions. SCGs will address challenges and maintain a current point of contact phone number for informally communicating a classification challenge and a current address to communicate formal classification challenges.

(2) A system for processing, tracking, and recording formal challenges to classification. The system used will differentiate the classification challenges with other reviews for possible declassification (for example, FOIA requests). Requests for information made under FOIA will be handled as directed by AR 25–55.

c. Policy and procedures regarding prescribed timelines for processing challenges, appeals, and challenges concerning RD/FRD are identified in DoDM 5200.01 and must be followed.

## **Section IV**

### **Security Classification Guides**

## **2–17. Policy**

An SCG will be issued for each system, plan, program, project, or mission which involves classified information. Agencies with OCA will prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides will conform to standards contained in this regulation and DoD regulations issued under DoDM 5200.01, Volume 1. DoDM 5200.45 provides detailed instructions on developing SCGs.

## **2–18. Content**

SCGs will identify specific items or elements of information to be protected and the classification level to be assigned each item or element. When deemed useful, specify the items or elements of information which are unclassified, or which were previously classified and now are declassified. Additional policies and procedures regarding the content of SCGs are found in DoDM 5200.01, Volume 1, DoDI 5200.48 and DoDM 5200.45.

## **2–19. Approval, distribution, and indexing**

a. SCGs will be personally approved in writing by an OCA who is authorized to classify information at the highest level designated by the guide, and who has program support or supervisory responsibility for the information or for the command's information security program.

b. SCGs will be distributed to those commands, contractors, or other activities expected to be derivatively classifying information covered by the guide.

c. Each approved SCG and its changes will be sent to the following agencies along with DD Form 2024 (DoD Security Classification Guide Data Elements):

(1) *Defense Office of Prepublication and Security Review, Washington Headquarters Service.* Guides that cover SCI or SAP information and that contain information that requires special access controls are exempt from this requirement. See AR 380–381 for guidance on distribution of classification guides for SAPs and AR 380–28 for guidance on SCI programs. The mailing address is: Defense Office of Prepublication and Security Review, 1155 Defense Pentagon, Washington, DC 20301–1155.

(2) *Army Declassification Activity.* One copy, in paper document (hard copy) and/or automated format (soft copy) will be sent. The mailing address is: Army Declassification Activity, 9301 Chapek Road, Building 1458, Fort Belvoir, Virginia 22060–5605. Email questions on how to send guides electronically to [usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-records-declassification@army.mil](mailto:usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-records-declassification@army.mil).

(3) *Defense Technical Information Center.* Provide one copy of each approved guide (including those issued as regulations, manuals, or other issuances, but not those covering Top Secret, SCI, or SAP information, or guides deemed by the guide’s approval authority to be too sensitive for automatic secondary distribution) to the Administrator, Defense Technical Information Center (DTIC), along with DD Form 2024. Each guide furnished to DTIC will bear the appropriate distribution statement required by DoDI 5230.24. The mailing address is: Defense Technical Information Center (DTIC–OA), Security Classification Guides, 8725 John J. Kingman Road, Fort Belvoir, VA 22060–6218. For information on email or electronic submission and preparation of the DD Form 2024, email [tr@dtic.mil](mailto:tr@dtic.mil).

(4) *Information security policy team.* Provide one copy of the approved guide along with the DD Form 2024 to DCS, G–2 (DAMI–CDS) by automated copy (soft copy) by contacting the information security policy team via email. Refer to <https://intelshare.intelink.gov/sites/hqda-odcs-g2-infosec>.

d. SCGs will be indexed in an online accessible index maintained by DTIC. The originator of the guide will submit DD Form 2024 to the Administrator, DTIC, upon approval of the guide. If the originator determines listing the guide in DTIC’s online database would be inadvisable for security reasons, issuance of the guide will be separately reported, with an explanation of why the guide cannot be listed, to the Director of Security, Office of the Under Secretary of Defense for Intelligence (OUSD (I)), along with a separate memorandum to DCS, G–2 (DAMI–CD).

e. Commands may access DTIC’s online SCG index by registering at <https://www.dtic.mil>.

## **2–20. Review, revision, and cancellation**

a. SCGs will be reviewed by the originator for currency and accuracy at least once every 5 years, or if concerning a defense acquisition program, prior to each acquisition program milestone, whichever occurs first. Changes identified in the review process will be promptly made. When a guide is revised, and a specific date was selected for declassification instruction, computation of declassification instructions will continue to be based on the date of the original classification of the information, and not on the date of the revision or reissuance. If no changes are required, the originator will advise the Administrator, DTIC, and DCS, G–2 (DAMI–CD) in writing, and the record copy of the guide will be so annotated with the date of review recorded on the new DD Form 2024.

b. Guides will be cancelled only when:

(1) All information specified as classified by the guide has been declassified;

(2) When the system, plan, program, or project classified by the guide has been cancelled, discontinued, or removed from the inventory and there is no reasonable likelihood that information covered by the guide will be involved in other classified programs or will be the subject of derivative classification; or

(3) When a major restructuring has occurred as the information is incorporated into a new classification guide and there is no reasonable likelihood that information covered by the guide will be the subject of derivative classification.

c. Impact of the cancellation on systems, plans, programs, and projects provided to other nations under approved foreign disclosure decisions, and impact of such decisions on existing U.S. SCGs of similar systems, plans, programs, or projects, will be considered in the decision. When an SCG is cancelled because the system, plan, program, or project has been cancelled, discontinued, executed, or removed from the inventory, the information covered by the guide is not automatically declassified. That decision rests with the OCA and authorized declassification authorities within the Army. Upon cancellation of a guide, the OCA, or other designated declassification official, with the concurrence of the OCA, will consider the need for publication of a declassification guide. In place of a separate declassification guide, declassification guidance can be included in a SCG for a similar, current system, plan, program, project, or mission.

d. Revision, reissuance, review, and cancellation of a guide will be reported to DTIC on DD Form 2024 as required for new guides. Copies of changes, reissued guides, and cancellation notices will be distributed as required for new guides as stated in paragraph 2–19.

## **Section V**

### **Nongovernment Research and Development Information**

#### **2–21. Policy**

Information that is a product of contractor or individual independent research and development (IR&D) or bid and proposal (B&P) efforts, as defined by DoDI 3204.01, conducted without prior or current access to classified information associated with the specific information in question may not be classified unless it meets all the requirements of EO 13526 and implementing directives, including this regulation. Additional policies and procedures regarding classification of this type of information are found in DoDM 5200.01, Volume 1.

## **Chapter 3**

### **Declassification, Downgrading, Upgrading, and Destruction**

#### **Section I**

##### **Army Declassification Program**

#### **3–1. General**

Permanent, historically valuable information will be declassified when it no longer meets the standards and criteria for classification in accordance with EO 13526. The authority to declassify information resides with the OCA for that information and those appointed as declassification authorities, subject to the criteria specified in EO 13526 or successor orders and implementing directives. DA files will not be declassified without prior review to determine if continued classification is warranted and authorized. EO 13526 contains provisions for four declassification programs as follows:

- a.* OCA declassification instructions at origination.
- b.* Automatic.
- c.* Mandatory.
- d.* Systematic.

#### **3–2. Special program manager**

*a.* The AASA is the Army's special program manager (SPM) for the execution of the centralized portion of the Army's automatic and systematic declassification program. The Army Declassification Activity (ADA) manages the Army's automatic and systematic declassification review program for the AASA, ensuring all requirements and deadlines associated with EO 13526, Sections 3.3 and 3.4, and its implementing directives are met. To ensure compliance, ADA also provides assistance, guidance, and training to ACOMs, ASCCs, and DRUs.

*b.* Acting as the SPM, the Chief, ADA will review those records subject to the automatic or systematic declassification provisions of EO 13526 located in National Archives and Records Administration facilities, to include the National Archives at College Park, MD; Washington National Records Center; and presidential libraries. The Chief, ADA will coordinate the declassification actions of DA commands subject to the automatic declassification program for records located in repositories other than the National Archives. Records stored at other locations will be reviewed by the command responsible for retiring the records, or by that command's successor in function, as appropriate. DA commands may also send their records to ADA for review, as necessary.

*c.* ACOMs, ASCCs, and DRUs will establish programs to ensure permanent, historically valuable records are reviewed prior to the date for automatic declassification and will provide the ADA with a letter of certification (LOC) concerning the automatic declassification review as stated in paragraph 3–10 (see fig 3–1).

*d.* For additional information about the ADA's mission, the ADA website address is <https://www.rmda.army.mil>.



DEPARTMENT OF THE ARMY  
ORGANIZATION  
STREET ADDRESS  
CITY STATE ZIP

OFFICE SYMBOL

xx XXX xxxx

CERTIFYING OFFICIAL (*Full name and position title of certifying official.*)

In accordance with AR 380-5, paragraph 3-2, the following information is provided regarding (your organization) compliance with the automatic and systematic declassification provisions of section 3.3 and 3.4 of Executive Order 13526 and the requirements specified in the Fiscal Years(s) 1999 and 2000 Defense Authorization Acts (Public Laws 105-26, Section 3161 and 106-65, Section 3149).

1. Total number of pages of permanently historical 25 year old and older records identified as subject to section 3.3 of EO 13526: (*page count here*).
2. Total number of pages reviewed under section 3.3 (automatic)
  - a. Total number of pages declassified: (*page count here*).
  - b. Total number of pages exempted: (*page count here*).
  - c. Total number of pages excluded: (*page count here*).
  - d. Total number of pages referred: (*page count here*).  
(Other Army or Federal agency information)
3. Total number of pages reviewed under section 3.4 (systematic): (*page count here*).
  - a. Total number of pages declassified: (*page count here*).
  - b. Total number of pages exempted: (*page count here*).
  - c. Total number of pages excluded: (*page count here*).
  - d. Total number of pages referred: (*page count here*).

CERTIFICATION: I, (*signature of certifying official here*)

On (*day, month, year*) certify that the records cited above have been reviewed in accordance with the automatic and systematic declassification provisions of Executive Order 13526, section 3.3 and 3.4 by a qualified declassification reviewer as stated in paragraph 3-10b.

Figure 3-1. Sample letter of certification

### **3–3. Declassification of Restricted Data and Formerly Restricted Data**

RD and FRD are not subject to EO 13526. This information is classified under the Atomic Energy Act of 1954, as amended. Declassification of RD and FRD information can only be accomplished with the express specific approval of the classification authority for the information. RD information can only be declassified by the DOE and FRD information can only be declassified jointly by DOE and DoD.

### **3–4. Declassification of other than Army information**

*a.* Records containing classified information that another government department or agency originated, other than records that are properly excluded or exempted from automatic declassification, will be referred to that agency prior to automatic declassification. ACOMs, ASCCs, and DRUs will identify other government department or agency information for referral during the initial review of records. The records will be referred using SF 715 (U.S. Government Declassification Review Tab) (Refer to <https://www.archives.gov/isoo/security-forms> for instructions on completing the SF 715.)

*b.* The ADA can provide additional information regarding recognizing the large number of equity holders.

## **Section II**

### **The Automatic Declassification System**

### **3–5. General**

*a.* EO 13526, Section 3.3, sets forth policy on the automatic declassification of information. Specifically, all classified records that are 25 years old or older determined to have permanent, historical value under 44 USC, will be automatically declassified whether or not the records have been reviewed. However, no DA records will be automatically declassified without review. DA records will be reviewed by an authorized declassification authority prior to 31 December of the year the records become 25 years old. As a result of the review, each record will be exempted, excluded, referred to another government department or agency or declassified, as appropriate. AR 25–400–2 identifies Army files determined to be of permanent, historical value under 44 USC. Agency records managers should be consulted in determining classified and permanent historical records holdings.

*b.* Permanent historical records may be reviewed when they reach 20 years of age.

*c.* The following provisions apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in EO 13526, that are otherwise subject to automatic declassification will not be automatically declassified until 31 December of the year that is 25 years from the date of the most recent record within the file block.

(2) Prior to automatic declassification, the command's declassification official may, in coordination with the Chief, ADA and Director, National Declassification Center, delay automatic declassification for up to 5 additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

(3) Prior to automatic declassification, the command's declassification official may, in coordination with the Chief, ADA and Director, ISOO, delay automatic declassification for up to 3 years for classified records that have been referred or transferred to that agency by another agency less than 3 years before automatic declassification would otherwise be required.

(4) The command's or organization's declassification official may, by coordination with the Chief, ADA and Director, ISOO, delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

*d.* Only records that have permanent, historical value under 44 USC are subject to automatic declassification. DA retention and destruction requirements apply to temporary records.

*e.* Automatic declassification does not constitute approval for public release of the information. Automatically declassified records will not be released to the public until a public disclosure review has been conducted.

### **3–6. Exemption from automatic declassification**

*a.* It is vital that sensitive DA information be protected from automatic declassification to ensure that current operations, systems, plans, and other information are not adversely affected. There are nine exemption categories specifically designated in EO 13526:

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

- (2) Reveal information that would assist in the development, production, or use of WMDs.
- (3) Reveal information that would impair U.S. cryptologic systems or activities.
- (4) Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system.
- (5) Reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans.
- (6) Reveal information, including FGI, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States.
- (7) Reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized.
- (8) Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security.
- (9) Violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.
- b.* For detailed exemptible Army information descriptions see the Army Declassification Guide (ADG) (25X/50X). The ADG is available to authorized automatic declassification reviewers. For questions concerning the ADG contact the ADA at [usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-records-declassification@army.mil](mailto:usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-records-declassification@army.mil).
- c.* Classified information that is determined to be sensitive may be exempted from automatic declassification for an additional 25 (25X), 50 (50X) or 75 (75X) years beyond the date of its origination if it falls within one of the exemption categories listed in this paragraph.
- d.* When 25-year-old information is determined to be exempt from automatic declassification, the information will remain classified until 31 December of the year that is 50 years from the date of origin. Prior to the date of automatic declassification, exempted records may be re-reviewed and exempted again for another 25 years, as appropriate. Currently, no further extension of classification past 75 years is authorized. If a record is re-reviewed and the DA information is determined to be declassified and it contains classified information that another government department or agency can exempt, it will be referred to those agencies. If the record is no longer exempt and does not contain classified information that another government department or agency can exempt, it will be declassified.
- e.* Exempting 25-year-old information (25X). An authorized declassification review official may exempt from automatic declassification specific 25-year-old information, the release of which should clearly and demonstrably be expected to reveal information described in one of the nine exemptions indicated above.
- f.* Exempting 50-year-old information (50X).
- (1) Information that is 50 years old may continue to be exempted from automatic declassification for an additional 25 years for a period not to exceed 75 years from the date of origin. The exemption category numbers are the same as for 25-year exemptions, except the number “50” will be used in place of “25.”
- (2) The ADG (25X/50X) authorizes exemption of specific information in the 50X1, 50X2, 50X4, 50X5, 50X6, and 50X8 exemption categories. (See the ADG (25X/50X) for details on these exemptions.)
- (3) Additionally, any information the release of which should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source (50X1–HUM), or key design concepts of a WMD (50X2–WMD) may be exempted from automatic declassification at 50 years. For definitions of a confidential human source or human intelligence source and key design concepts of WMDs, consult the ADG (25X/50X).
- g.* Currently, the Army is not authorized to exempt 75-year-old information (75X).
- h.* The Army is not currently authorized to apply a file series exemption (FSE). However, ACOMs, ASCCs, or DRUs may request authorization of an FSE, as appropriate. All such requests for FSE authorization will be coordinated with the Chief, ADA.
- i.* As new information that qualifies for exemption from automatic declassification is identified, it must be reported to the ADA for inclusion in the ADG. An unclassified description of the information proposed for exemption and the reason the information must remain classified beyond 25 years must be included in the proposed exemption memorandum to ADA. The ADG will be updated at least every 5 years but may be updated more frequently, as necessary.
- j.* Information exempted from automatic declassification remains subject to the mandatory and systematic declassification review provisions of this regulation.

### **3–7. Marking records exempted from automatic declassification**

- a.* Records that contain information exempted from automatic declassification at 25 years will be marked with the designation “25X,” followed by the number of the exemption category and a declassification date or event. For example, a record originated in 1988 is reviewed at 25 years (2013). If it contains information that requires continued



classification because of exemption category 4, “Reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system,” the new automatic declassification date will be 31 December 2038 (1988 + 50 = 2038). The declassification marking would be written as “Declassify On: 25X4, 20381231.”

b. Records that contain information previously exempted from automatic declassification at 50 years will be marked with the designation “50X,” followed by the number of the exemption category and a declassification date or event. For example, assume the record cited above, which was originated in 1988, is re-reviewed in 2038 and the information requires continued classification per the ADG (25X/50X). In this case, the new automatic declassification date will be 31 December 2063 (1988 + 75 = 2063). The new automatic declassification marking would be written “Declassify On: 50X4, 20631231.”

### **3–8. Records review guidelines**

a. *Exempt, exclude, refer, or declassify.* Each record subject to automatic declassification will be thoroughly reviewed on a page-by-page basis and one of four possible disposition decisions will be applied. The four automatic declassification disposition decisions are: exempt, exclude, refer, or declassify. A concurrent release review is not required for records subject to automatic declassification, but must be performed before public release.

(1) *Exempt.* Records are exempted at 25 or 50 years when they clearly contain information that fall under one or more of the exemption categories in paragraph 3–6. Specific application of these exemptions is provided in the ADG (25X/50X).

(2) *Exclude.* Records containing RD and/or FRD markings are excluded from automatic declassification in accordance with EO 13526. However, when unmarked RD information is identified in a record, it is referred to DOE. Unmarked FRD is referred to DOE and the Deputy Assistant Secretary of Defense for Nuclear Matters. See 50 USC 2672, which addresses requirements for protecting against the inadvertent release of RD and FRD records subject to automatic declassification under EO 13526.

(3) *Refer.* Referrals to other government departments or agencies are made only after reviewing for exclusions or Army exemptions. Records for which there is no DA objection to declassification but which contain classified information that another government department or agency can exempt, will not be declassified by the DA. These records are referred to the appropriate government department(s) or agency(s). Commands are not authorized to declassify information from other government departments or agencies or from other commands. Records that contain information another government department or agency or command can exempt will be referred to the identified government departments or agencies and reported to ADA. Information from other commands can either be referred to the identified agency or sent to ADA for review, as appropriate.

(4) *Declassify.* DA-originated records are declassified when they do not contain information falling under the exemption categories specified in paragraph 3–6, do not contain classified information that another government department or agency can exempt, and do not contain RD or FRD.

b. *Tabbing records.* When stamping records is not possible, agencies will use the SF 715 to tab all exempt, excluded, and referred records. DA records that are declassified do not need to be tabbed. Reviewers that fail to complete the SF 715 in a legible and clear manner place their content at risk. The SF 715 may be ordered through the Government Publishing Office (GPO).

c. *Stamping records.* Commands that conduct automatic declassification reviews of records in their custody/logistical control should stamp records or use SF 715s prior to accessioning. See Section 25, Part 2001, Title 32, Code of Federal Regulations (32 CFR 2001.25) for instructions on marking a declassified record. For excluded, exempted, or referred records, use the information fields from the SF 715, as applicable.

d. *Pre-1946 records.* Most DoD classified information that originated prior to 1 January 1946 was declassified with the exception of information in specific categories. Agencies will contact the ADA for further guidance in review and declassification of information of this type.

### **3–9. Army commands, Army service component commands, direct reporting units requirements**

Commanders of ACOMs, ASCCs, and DRUs that maintain physical custody/logistical control of federal records subject to the automatic declassification requirements of the EO will:

- a. Identify 25-year-old and older permanent, historical records subject to automatic declassification.
- b. Ensure personnel who review records for automatic declassification have completed the ADA’s Automatic Declassification Reviewers training course and DOE’s Historical Records Restricted Data Reviewers Course if records are likely to contain RD/FRD.
- c. Review records subject to EO 13526 or coordinate the review with the ADA.

d. Report the status of their reviews to the ADA by completing the annual ADA LOC by 31 December of each year (see fig 3–1). The LOC will be signed by the command’s declassification official, or their designee. Negative responses are required.

e. Provide a proposal to exempt Army information in memorandum form to the ADA for inclusion in the ADG (25X/50X) when proposing to exempt information not already specified in the ADG.

## **Section III**

### **Mandatory Declassification and Systematic Declassification Reviews**

#### **3–10. Mandatory declassification reviews**

a. Any individual or organization may request a mandatory declassification review (MDR) of information classified under EO 13526, or predecessor orders. Upon receipt of such a request, the responsible command will conduct a review if:

(1) The written request describes the record or material with sufficient specificity to allow it to be located with a reasonable amount of effort;

(2) The information is not exempt from search and review under the National Security Act of 1947;

(3) The information is not classified under the Atomic Energy Act of 1954, as amended.

b. Information originated by the incumbent President, the incumbent President’s White House Staff, committees, commissions, or boards appointed by the incumbent President, or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempt from the provisions of this section.

c. The DCS, G–2, is the DA proponent for MDR requests; however, the ADA serves as a centralized point of contact and coordinates all requests from the Washington Headquarters Services and the Presidential Libraries. Since the ADA is not a repository for records, all MDR requests received are forwarded to the agency having cognizance of the information. Forwarded requests will include instructions for responding directly to the requester.

(1) ACOMs, ASCCs, DRUs, and AASA will establish systems for promptly responding to requests for MDR. Information will be reviewed on a line-by-line basis and declassified if it no longer meets the standards for classification. Information that is declassified will be released to the requester unless withholding is appropriate under applicable law (for example, FOIA or Privacy Act of 1974).

(2) If records reviewed for declassification under this section contain information that has been originally classified by another DoD Component or Executive Branch agency, the reviewing activity will refer the appropriate portions of the request to the originating organization. Unless the association of that organization with the requested information is itself classified, the Army agency that received the request may notify the requester of the referral. Any FGI will be referred to the Department of State.

(3) If the requested information has been reviewed for declassification within the 2 years preceding the request, or if the information is subject to pending litigation, the DA command will notify the requester and provide appeal rights. No additional review is required.

(4) The requester should receive a final determination response from the agency within 1 year of the request; otherwise the requester has the right to appeal directly to the Interagency Security Classification Appeals Panel (ISCAP).

#### **3–11. Mandatory declassification review appeals**

a. The MDR Program provides for an administrative appeal in cases where the review results in the information remaining classified. The requester will be notified of the results of the review and of the right to appeal the denial of declassification. The requester must first appeal the MDR with the denying agency’s appellate authority. The appeal must be filed within 60 days of receipt of denial from the agency.

b. If the appeal is denied, the appellate authority must notify the requester of the right to appeal the denial to the ISCAP. The requester must file the appeal within 60 days.

c. The Office of the General Counsel is the Army’s MDR appellate authority.

#### **3–12. Systematic declassification reviews**

a. Systematic declassification review is conducted at the interagency level at the National Declassification Center.

b. ACOMs, ASCCs, and DRUs that have 25-year-old and older permanent historical records that were previously reviewed and exempted in accordance with EO 13526, Section 3.3, or predecessor orders should contact ADA for guidance for reviewing these records.

## Section IV

### Change in the Level of Classification

#### 3–13. General

OCAs may change the level of classification (upgrade or downgrade) of information under their jurisdiction, provided the information continues to meet the standards for classification identified in this regulation and EO 13526. When doing so, OCAs will update SCGs where appropriate and notify all known holders of the information of the changes (see para 2–19 for processing SCGs). Downgraded and/or upgraded information will be re-marked in accordance with DoDM 5200.01, Volume 2.

#### 3–14. Downgrading

*a.* Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level and can be properly protected at a lower level. The principal purpose of downgrading is to conserve security resources by avoiding protection of information at too high a level.

(1) *Downgrading decisions during original classification.* Downgrading should be considered when OCAs are deciding on the duration of classification to be assigned. If downgrading dates or events can be identified, they must be specified along with the declassification instructions. Note that downgrading instructions do not replace declassification instructions.

(2) *Downgrading at a later date.* Information may only be downgraded by the OCA or a designated declassification official. The OCA making the downgrading decision will notify holders of the change in classification.

*b.* OCAs may designate members of their staffs to exercise declassification authority over information under their jurisdiction and must receive training as outlined in chapters 3 and 9.

#### 3–15. Upgrading

Classified information may be upgraded to a higher level of classification only by officials who have been delegated the appropriate level of OCA. Information may be upgraded only if holders of the information can be notified of the change so that the information will be uniformly protected at the higher level. The OCA making the upgrading decision is responsible for notifying holders of the change in classification.

## Section V

### Classified Material Destruction Standards

#### 3–16. General

Classified documents and material will be destroyed completely to preclude recognition or reconstruction of the classified information contained in or on the material. National Security Agency (NSA)/Central Security Service (CSS)-approved destruction methods include burning, crosscut shredding, wet-pulping, melting, mutilation, chemical decomposition, and pulverizing. Methods used for clearing, sanitizing, or destroying classified information technology (IT) equipment and media include overwriting, degaussing, sanding, and physical destruction of components of media. Classified information identified for destruction will continue to be protected as appropriate for its level of classification until destroyed.

*a.* COMSEC material will be destroyed in accordance with AR 380–40.

*b.* North Atlantic Treaty Organization (NATO) material will be destroyed as outlined in USSAN 1–07.

*c.* FGI will be destroyed in the same manner as U.S. classified information of the equivalent level, except where otherwise required by international treaty or agreement. See paragraph 5–19 for further guidance on safeguarding FGI and requirements of recording destruction of FGI material.

#### 3–17. Approved routine methods of destruction

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. The EPLs may be obtained by visiting <https://www.nsa.gov/resources/everyone/media-destruction/>.

*a.* 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.

*b.* In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly (for example, shredder blade assembly), the unit must be replaced with one listed on the current appropriate EPL.

- c. Classified IT storage media (for example, hard drives) cannot be declassified by overwriting. Sanitization (which may destroy the usefulness of the media) or physical destruction is required for disposal.
- d. For guidance on clearing, purging (sanitizing), destroying, or disposing of information system (IS) media, refer to AR 25–2.
- e. Storage media containing SCI will be handled as stated in AR 380–28. SAPs will be handled in accordance with AR 380–381.

### **3–18. Technical advice on approved destruction devices and methods**

Contact the NSA/CSS System and Network Analysis Center via email at [snac@radium.ncsc.mil](mailto:snac@radium.ncsc.mil) to obtain technical guidance concerning appropriate methods, equipment, and standards for destroying classified electronic media, IS equipment, electronic components, and other similar or associated materials.

a. *Crosscut shredders.* Only crosscut shredders listed on the NSA/CSS EPL for High Security Crosscut Paper Shredders may be used to destroy classified material by shredding. When COMSEC material is destroyed by shredding, only crosscut shredders listed in NSA/CSS Specification 02–01 at the time of acquisition will be used. Refer to AR 380–40 for destruction requirements for COMSEC material.

(1) Pending replacement, commanders of ACOMs, ASCCs, and DRUs will ensure that procedures are in place to manage the risk posed by using crosscut shredders not on the approved NSA/CSS list. At a minimum, the volume and content of each activity’s classified material destruction flow will be assessed and a process established to optimize the use of high security crosscut paper shredders (for example, with Top Secret collateral material being the highest collateral priority) to take full advantage of the added security value of those shredders.

(2) The bag of shredded material will be “stirred” before discarding to ensure that the content is mixed up.

(3) 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 EPL 02–02” for High Security Disintegrators 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.

## **Chapter 4**

### **Controlled Unclassified Information**

#### **4–1. General**

a. CUI, though not classified under EO 13526, requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies in accordance with EO 13556 and DoDI 5200.48.

b. DA personnel will follow the policy and procedures outlined in DoDI 5200.48 as it relates to the designation, protection, destruction, and decontrol of CUI.

c. Documents and material containing CUI will be marked in accordance with DoDI 5200.48.

## **Chapter 5**

### **Access, Control, Safeguarding, and Visits**

#### **Section I**

#### **Access**

##### **5–1. Responsibilities**

DA personnel are personally responsible for safeguarding classified information and material. This responsibility includes ensuring they do not permit access to classified information and material by unauthorized personnel. Both the security clearance eligibility and the need-to-know must be present before access is authorized. The holder of the information, not the potential recipient, must confirm valid need-to-know and must verify the level of security clearance eligibility or access authorization. Collecting, obtaining, recording, or removing any classified material or information for any personal use whatsoever is prohibited.

##### **5–2. Nondisclosure agreement**

a. Prior to granting access to classified information, DA personnel will receive a briefing on their responsibility to protect classified information and will sign SF 312 (Classified Information Nondisclosure Agreement) (also known

as an NDA) or other NDA approved by the Director of National Intelligence (DNI). Electronic signatures will not be used to execute the SF 312.

*b.* Contractor personnel will execute the NDA through their company and not through the sponsoring DA command unless working as a consultant for that agency.

*c.* Non-U.S. Government personnel, who have been hired under civil service procedures as consultants to the DA, and granted security clearance eligibility and access, will follow the same procedures as stated in paragraph 5-2*a*.

*d.* SCI and SAP access requirements will be completed in accordance with AR 380-28 and AR 380-381 respectively, for those meeting requirements of access to classified information stated in paragraph 5-2*a*.

### **5-3. Signing and filing the nondisclosure agreement**

*a.* Once the NDA has been executed, a command official will witness the execution of the NDA by signing and dating the form immediately after the individual's signature. The same official, or another official in the command who witnesses the form, can serve as the accepting official. Once completed, the date will be recorded in the Defense Information System for Security (DISS), or its successor system of record, in accordance with AR 380-67. Original copies will be kept on file in the individual's official personnel folder (OPF). SF 312 will be retained for 50 years from the date of signature. See AR 600-8-104 and U.S. Office of Personnel Management guide "The Guide to Personnel Recordkeeping" operating manual for filing instructions.

*b.* The SM or other command official will coordinate final disposition of the SF 312 with their local personnel offices (for example, military personnel office for Soldiers, civilian personnel advisory centers for civilian personnel) to ensure the SF 312 is properly filed and maintained in the individual's OPF, applying the appropriate disposition instructions.

*c.* If a consultant to the DA is hired under civil service procedures, as opposed to contracting with a company for consultant services, the NDA will be executed and filed as for DA personnel. If the consultant's OPF is not retired, the command is obligated to retain the NDA for the required 50-year retention period. Consultant NDAs cannot be used by or transferred to another activity. They only authorize access to classified information under a specific agreement and access termination must be executed when the agreement has ceased or when classified access is no longer required, whichever occurs first. In special situations where nongovernment uncleared personnel have been granted classified access to specific information in accordance with the policy established in AR 380-67, the NDA will be attached to the exception to policy memorandum or other appropriate written authorization which authorizes the individual's access to classified information and will be retained in the command's files for the required retention period of 50 years.

### **5-4. Refusal to execute the nondisclosure agreement**

If a person refuses to sign the NDA, he or she will not be permitted access to classified information and an incident report will be submitted as required by AR 380-67.

### **5-5. Debriefing and termination of classified access**

*a.* Classified information is not the personal possession of any DA personnel, regardless of rank, title, or position. Classified information will not be removed to nonofficial or unapproved locations, such as personal residences, upon the termination of employment or military service of any person, including the custodian of that material.

*b.* All DA personnel who are retiring, separating, resigning, being discharged, or who will no longer have access to classified information, will out-process through the command security office or other designated command office and receive a termination briefing. During this out-processing, the individual will be informed that access to classified information has been terminated and the individual still has an obligation to protect any knowledge they have of classified information. These individuals will sign a security termination statement at the time of out-processing. The "Security Debriefing Acknowledgement" section of an SF 312 will be used for this purpose. This does not require the individual's originally signed SF 312. The security termination statement (SF 312) will be maintained in the command's security office, or other designated command office, for a period of 2 years, in accordance with AR 25-400-2 and AR 380-67.

*c.* DA personnel who refuse to sign the security termination statement as stated in paragraph 5-5*b*, will be reported as required by AR 380-67.

*d.* The same procedures will be followed for DA personnel still employed and still in service whose security clearance eligibility has been withdrawn, denied (after interim access was granted), or revoked either for cause or for administrative reasons due to lack of need for future access to classified information. In these cases, individuals will execute the debriefing statement as stated in paragraph 5-5*b*.

*e.* Unless exempted by the senior security official at the ACOM, ASCC, or DRU level, security out-processing is required for all cleared personnel transferring to another DA command or to a federal government agency. Transfers will not require the execution of the type of debriefing statement described in paragraph 5–5*b*. This does not preclude the command from requesting the transferring individual sign or initial a form or statement indicating, in substance, that the individual has been advised of the continuing responsibility to protect classified information and/or has completed the security out-processing. Personnel transferring will be briefed on the responsibilities stated in paragraph 5–5*b*.

*f.* Out-processing can also be used as a means to ensure that the appropriate command security officials are aware of the departure of personnel to ensure combinations and passwords are changed, keys are returned, and accountable documents and property are under new custody. Where out-processing is not required for transfers, the command will establish procedures to ensure the SM is advised of such transfers.

*Note.* There is no requirement to execute a new NDA when access is removed from DISS, or its successor system, during out-processing based on a transfer to another command. Debriefings will be completed and maintained on file for a minimum of 2 years, in accordance with AR 25–400–2.

## **5–6. Access to Restricted Data, Formerly Restricted Data, and critical nuclear weapon design information**

*a.* Access to RD and FRD, including critical nuclear weapons design information (CNWDI) by DA personnel at Army facilities, will be under the same conditions of a comparable level of security classification, based on the appropriate security clearance eligibility and access, need-to-know for the information, and in accordance with DoDI 5210.02.

*b.* Access to CNWDI is strictly limited to U.S. citizens. In rare cases, an exception to the U.S. citizenship requirement will be made. This determination will be made by the Secretary of Defense based upon the recommendation of the SECARMY. Such requests will be forwarded through command channels to DCS, G–2 (DAMI–CD).

## **5–7. Access by persons outside the Executive Branch**

*a. General.* Classified information can be made available to individuals or agencies outside the Executive Branch, provided such information is necessary for performance of a lawful and authorized function and with the approval of the originating department or agency. The SECARMY; DCS, G–2; or commanders of ACOMs, ASCCs, DRUs, and the AASA are designated as DA release authorities, unless otherwise specified in this regulation. They are authorized to determine, subject to OCA approval and before the release of classified information, the propriety of such action in the interest of national security and the assurance of the recipient’s trustworthiness and need-to-know. This authority can be further delegated, if required, unless otherwise specified in this regulation.

### *b. Congress.*

(1) Congressional staff members requiring access to DoD classified information will be processed for a security clearance in accordance with DoDI 5400.04.

(2) The Assistant Secretary of Defense (Legislative Affairs), as the principal staff assistant to the Secretary of Defense responsible for DoD relations with members of Congress, will provide for DoD processing of personnel security clearances for members of Congressional staffs.

(3) Personnel testifying before a Congressional committee in executive session or in relation to a classified matter will obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of information that is to be presented.

*c. Government Publishing Office.* Documents and material of all classification may be processed by GPO, which protects the information in accordance with the DoD/GPO Security Agreement.

*d. Government Accountability Office.* Representatives of the Government Accountability Office (GAO) can be granted access to classified information, originated by and in the possession of the DA and DoD, when such information is relevant to the performance of the statutory responsibilities of that office, as set forth in DoDI 7650.01. Certifications of security clearance, and the basis thereof, will be accomplished pursuant to arrangements between GAO and the concerned command. Personal recognition or presentation of official GAO credential cards is acceptable for identification purposes but is insufficient for access to classified information.

*e. Historical researchers.* Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to DoD classified information provided that the SECARMY, the DCS, G–2, commanders of ACOMs, ASCCs, DRUs, or the AASA, with the concurrence of the OCA responsible for classifying the information, completes the requirements stated in DoDM 5200.01, Volume 3. This authority cannot be further delegated.

Security clearance eligibility requirements contained in AR 380–67 will be followed and an NDA must be executed and maintained for the required period of time.

*f. 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 be authorized access to classified information they originated, reviewed, signed, received, or that was addressed to them while serving as an appointee or designee in DoD, provided that the SECARMY or the DCS, G–2, with concurrence of the OCA responsible for classifying the information, completes the requirements stated in DoDM 5200.01, Volume 3.

*g. Judicial, nonjudicial, or administrative proceedings.* Persons outside the executive branch may only be authorized access to classified information for the purposes of preparing for or participating in a judicial, nonjudicial, or administrative proceeding as authorized by the OCA who originally classified the information. Release of classified information to such persons must be consistent with the applicable provisions of DoDD 5405.2 and AR 27–40. Release of classified information to such persons in judicial or nonjudicial proceedings conducted under the Uniform Code of Military Justice will also be in accordance with AR 27–10 and Military Rule of Evidence 505. All persons outside the executive branch who have been determined by the OCA who classified the information to have a need for such access must obtain security clearance eligibility and sign an NDA in accordance with DoDM 5200.02 and AR 380–67 prior to being granted such access. Persons who represent a party whose interests are adverse to the interests of the United States will be considered to be persons outside the Executive Branch for purposes of obtaining access to classified information to prepare for or participate in a judicial, nonjudicial, or administrative proceeding regardless of whether such persons are employed by the DoD or are performing duties as a member of the armed services.

*h. Special cases.* When necessary, in the interests of national security, commanders of ACOMs, ASCCs, and DRUs, and the AASA may request through the DCS, G–2, that access to classified information by persons outside the federal government be granted, other than those identified above. Requests must be processed and approved in accordance with the provisions of DoDM 5200.01, Volume 3.

## **Section II**

### **Control Measures and Visits**

#### **5–8. Responsibilities**

*a.* Commands will maintain a system of control measures that ensures access to classified information is limited only to authorized persons. The control measures will be appropriate to the environment in which the access occurs and the nature and volume of the information. The system will include technical, where appropriate, physical, administrative, personal, and personnel control measures. This includes information created, stored, transmitted, or deleted in IT systems.

*b.* Classified information will be protected at all times, either by storage in a General Services Administration (GSA)-approved security container or having it under the personal observation and physical control of an authorized individual.

#### **5–9. Care during working hours**

*a.* Classified material removed from storage will be kept under constant surveillance and control by authorized personnel. Classified document cover sheets, SF 703 (Top Secret Cover Sheet (orange)), SF 704 (Secret Cover Sheet (red)), or SF 705 (Confidential Cover Sheet (blue)), will be placed on classified documents or files not in security storage. All items containing classified information, such as drafts, carbons, notes, electronic media, typewriter and printer ribbons, plates, stencils, and worksheets, will be destroyed immediately after they have served their purpose or protected as required for the level of classified information they contain.

*b.* SF 702 (Security Container Check Sheet) will be displayed conspicuously on each piece of GSA-approved equipment used to store classified material. The SF 702 need not be used for facilities secured by high security locks, provided the key and lock control register provides an audit capability in the event of unsecured facilities. SF 702 is used to record the date and time of each instance when a security container is opened and secured (locked). The following procedures apply:

(1) Properly cleared personnel will record the date and time whenever they unlock or lock the security equipment during the day followed by their initials.

(2) If a GSA-approved security container is locked, and the room in which it is located is to be left unattended, whenever possible, a person, other than the person who locked the container, will check the container to make sure it is properly secured. The person doing the checking will record the time the container was checked and initial the form.

The person who locked the container will see that the check is made. If this is not possible, the same person locking the safe will initial the form as being checked.

(3) Containers not opened during a workday will be checked and the action recorded as in paragraph 5–9b.

(4) Notations will also be made on SF 702 if containers are opened after-hours, on weekends, and on holidays, as provided above. All days in the month will be accounted for on the SF 702 regardless if checks were made during nonduty hours or holidays.

c. Reversible “OPEN–SECURED” signs will be used on each security container, secured area, or vault in which the level of classified information is stored. Signs are available free of charge through the DoD Lock Program available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).

d. A person discovering a security container or security storage area open and unattended will:

(1) Keep the container or area under guard or surveillance.

(2) Notify one of the persons listed on SF 700 (Security Container Information), Part 1, affixed to the inside of the security container lock drawer. If one of these individuals cannot be contacted, the duty officer, SM, or other appropriate official will be notified.

e. Individuals contacted when a container or area is found open or unattended will—

(1) Report personally to the location; check the contents of the container or area for visible indications or evidence of tampering, theft, or compromise. If any evidence of tampering, theft, or compromise is noted:

(a) Installation or activity security personnel (if not at the scene) will be immediately notified so a preliminary investigation can be initiated.

(b) The custodian will cease examination of the container and its contents (to prevent destruction of physical evidence) unless otherwise instructed by security personnel.

(c) A GSA certified inspector will be called to determine the nature of the tampering and whether the security container is operating properly.

(2) Change the combination and lock the container. If the combination cannot be changed immediately, the security container will be locked and placed under guard until the combination can be changed, or the classified contents will be transferred to another container or secure area.

(3) If not previously accomplished, report the incident to the commander or SM immediately for action relative to compromise or possible compromise.

## **5–10. End-of-day security checks**

a. Commands that access, process, or store classified information will establish a system of security checks at the close of each working day to ensure that all classified material is properly secured. SF 701 (Activity Security Checklist) will be used to record these checks. An integral part of the security check system will be the securing of all vaults, closed areas or secure rooms, and containers used for the storage of classified material; SF 702 will be used to record such actions. In addition, SF 701 and SF 702 will be annotated to reflect after-hours, weekend, and holiday activity. SF 701 and SF 702 will be held for 90 days following the last entry or longer if part of an ongoing investigation.

b. After-duty-hours security checks of desks may be conducted provided:

(1) DA personnel are notified of local policy and procedures pertaining to after-hours inspections; locking of desks, file, or storage cabinets; and maintenance of duplicate keys or combinations. Notification must be in writing and in advance of any after-hours inspection program.

(2) After-duty-hours inspections are conducted only by security personnel, and for the sole purpose of detecting improperly secured classified information.

## **5–11. Emergency planning**

Commands will develop plans for the protection, removal, and destruction of classified material in case of fire, natural disasters, civil disturbance, terrorist activities, or enemy action to minimize the risk of its compromise. The level of detail in the plan and the amount and frequency of testing of the plan is the command option, subject to ACOM, ASCC, or DRU approval, and should be based upon an assessment of the risk, which might place the information in jeopardy. In this regard, special concern will be given for locations outside the United States.

a. In preparing emergency plans, consideration must be given to the following:

(1) Reducing the amount of classified material on hand;

(2) Creating regular backup copies in electronic formats by authorized means for offsite storage.

(3) Transferring as much retained classified information to electronic media, by authorized means, as possible.

b. AR 380–40 contains policy for the emergency protection, including emergency destruction under no-notice conditions, of COMSEC material.



c. Post emergency plans in a highly visible area, in the vicinity of all personnel. Emergency planning should be a collaborative effort and reviewed by contributing departments within the command.

#### **5-12. Classified discussions**

a. Classified discussions are not permitted in personal residences, in public, in public transportation conveyances (airplane and taxi), or in any area outside approved spaces in a government or cleared contractor facility except as discussed in paragraph b below. Classified information will only be discussed, in telephone conversations, over secure communications equipment, such as secure terminal equipment (STE), and circuits approved for transmission of information at the level of classification being discussed.

b. When discussing classified information, the ability of others in the area (who are not appropriately cleared or do not have a need-to-know) to hear the conversation will be taken into consideration. This includes instances where the installation of STE telephones are authorized in personal residences in accordance with paragraph 6-6.

#### **5-13. Removal of classified storage and information technology equipment**

Storage containers and IT equipment which had been used to store or process classified information will be inspected by cleared personnel before removal from protected areas and/or before unauthorized persons are allowed unescorted access to them. The inspection will ensure that no classified information remains within or on the equipment. Items to be inspected include security containers, reproduction equipment, facsimile machines, micrographic readers and printers, IS equipment and components, equipment used to destroy classified material, and other equipment used for safeguarding or processing classified information. A written record of the inspection will be completed and maintained in accordance with paragraph 6-11.

#### **5-14. Visits**

Commands will establish procedures to control access to, or disclosure of, classified information by visitors. At a minimum, local procedures will include the identity, security clearance eligibility, access, if appropriate, and the need-to-know for all visitors.

a. Visit requests will be processed and security clearance eligibility and access level verified in accordance with AR 380-67.

b. Official visits by foreign government representatives to DA commands will be handled in accordance with AR 380-10.

#### **5-15. Classified meetings and conferences**

Meetings and conferences, which include classes, seminars, symposia, and similar activities, at which classified information is to be presented or discussed, are considered classified meetings. The classified portions of these meetings present vulnerabilities to unauthorized disclosure and will be limited to persons possessing an appropriate security clearance, access, and the need-to-know for the specific information involved. Security requirements contained elsewhere in this regulation and other applicable security regulations apply, without exception, to classified meetings.

a. Commanders of ACOMs, ASCCs, DRUs, or the AASA will ensure that approval processes for classified meetings meet the following requirements:

(1) The classified meeting or session is mission critical to the Army.

(2) Use of other approved methods or channels for disseminating classified information or material are insufficient, impractical, and not cost effective.

(3) The meeting, conference, or classified sessions take place only at an appropriately cleared government facility or a contractor facility that has an appropriate facility security clearance and, as required, secure storage capability, unless a waiver is approved in advance by the DCS, G-2.

(a) Requests for waivers to permit use of facilities other than appropriately cleared U.S. Government or U.S. contractor facilities will be submitted through the organization's ACOM, ASCC, DRU, or the AASA, in writing for approval to the DCS, G-2 (DAMI-CDS) a minimum of 45 days prior to the classified meeting. Requests will be sent by secure internet protocol router network (SIPRNET).

(b) The request will include a security plan that outlines how the requirements of paragraphs 5-15b and 5-15d are being met.

(4) If a classified meeting or conference is held at a cleared U.S. contractor location, the contractor will comply with all applicable portions of DoDM 5220.22 and 22 CFR Parts 120 through 130 (also known as the International Traffic in Arms Regulations). DCS, G-2, approval for the conduct of the meeting does not constitute authorization for presentation of export-controlled information when foreign nationals attend.

(5) The conduct of classified meetings or conferences at foreign installations and foreign 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, ACOM, ASCC, DRU, or the AASA will 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 regulation and other related DA and DoD regulations. The provisions of paragraph 5–15*d* also will be satisfied. Assistance can be provided by the Director, International Security Directorate, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy (OUSD (P)) through DCS, G–2 (DAMI–CDS).

(6) Routine day-to-day classified meetings and gatherings at DA commands will be conducted only at an appropriately cleared government or contractor facility. Waivers will not be granted for routine meetings.

(7) The provisions of this section do not apply to operational meetings conducted in combat situations, classes conducted by DA schools, or gatherings of personnel of a DA command and foreign government representatives or U.S. and/or foreign contractor representatives on a matter related to a specific government contract, program, or project.

(8) Classified sessions are segregated from unclassified sessions.

(9) 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.

(10) Any participation by foreign representatives complies with requirements of AR 380–10.

(11) Announcement of a 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.

(12) ISs used during the meeting or conference to support creation or presentation of classified information will meet all applicable requirements for processing classified information in accordance with AR 25–2, including, as appropriate, considerations of technical security countermeasures (TSCM). Unclassified laptop computers, handheld information technologies (for example, personal electronic devices (PEDs)), and other similar devices capable of recording or transmitting will not be used for note taking during classified sessions. Use of classified computers and other electronic devices will be permitted only when needed to meet the intent of the meeting or conference and applicable protection and TSCM requirements have been met.

*b.* The DA command sponsoring a classified meeting or conference will assign an official to serve as SM 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 only authorized personnel gain entry to the area.

(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 (for example, setting up food or cleaning) when classified presentations and/or discussions are not in session.

(5) Use of cell phones, PEDs, two-way pagers, laptop computers and other electronic devices that record or transmit is prohibited.

(6) Classified notes and handouts are safeguarded in accordance paragraph 5–9 of this regulation.

(7) Classified information is disclosed to foreign government representatives only in accordance with the provisions of AR 380–10.

(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 government contractor personnel may provide administrative support and assist in organizing a classified meeting or conference, but the DA command sponsoring the gathering remains responsible for all security requirements.

*d.* Facilities other than appropriately cleared government or U.S. contractor facilities proposed for use for classified meetings and conferences will:

(1) Not be open to the public and access will 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 installation, 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 this chapter of the regulation.

(4) Meet the DoD antiterrorism standards specified in AR 525–13.

(5) Be subject to TSCM surveys in accordance with DoDI 5240.05. 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 command will provide an after-action report to the DCS, G-2 (DAMI-CDS). The after-action report will be a brief summary of any issues or threats encountered during the event and actions taken to address the situation.

### **Section III**

#### **Accountability and Administrative Procedures**

##### **5-16. Equipment used in information technology networks**

There is 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. Command IT-certified technicians will identify those features, parts, or functions of equipment used to process classified information that may retain some or all of the information. Command security procedures will prescribe the appropriate safeguards to prevent unauthorized access to that information and replace, control, and/or destroy equipment parts, pursuant to the level of the classified material contained therein prior to disposal. Alternatively, the equipment can be designated as classified and appropriately protected at the retained information's classification level (for instance, by being re-installed in a secure area approved for the storage of classified information at the appropriate classification level for the material).

##### **5-17. Receipt of classified material**

Commands will develop procedures to protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is contained in the mail. Screening points will be established to limit access to classified information.

##### **5-18. Top Secret information**

Top Secret control and accountability is not mandatory, but if the commander elects to appoint a Top Secret control officer (TSCO) to facilitate appropriate control of Top Secret material, procedures for the control and accountability of the Top Secret material will be developed. These procedures should provide the means of facilitating oversight and management of Top Secret access controls, assessment and management of holdings, and identification of material at risk in cases of potential unauthorized disclosure. In developing these procedures, the following requirements will be met.

*a.* TSCOs and one or more alternates will be designated in writing and will be responsible for receiving, dispatching, and maintaining accountability and access records for Top Secret material. Such individuals will be selected on the basis of experience and reliability and, as a general rule, will already possess the appropriate security clearance eligibility and access equal to or higher than the information to be handled. TSCOs will maintain a current, accurate system of accountability within the command for all Top Secret documents and other material. TSCOs will record the receipt, dispatch, downgrading, movement from one command element to another, current custodian, and destruction of all Top Secret material.

*b.* Top Secret material will be accounted for by a continuous chain of receipts. Receipts will be maintained for 5 years. Top Secret registers and Top Secret accountability record forms (for example, DA Form 3964 (Classified Document Accountability Record)) or equivalent will reflect sufficient information to identify adequately the Top Secret document or material.

*c.* At a minimum, the register should include the title or short title, date of the document, identification of the originator, copy number, and disposition. Top Secret material will be numbered serially and marked to indicate its copy number (for example, copy 1 of 2 copies) and accounted for accordingly.

*d.* Top Secret material will be inventoried at least once annually. The inventory will reconcile the Top Secret accountability register and records with 100 percent of the Top Secret material held. The inventory will be conducted by two properly cleared individuals. One will be the TSCO or alternate, and the other will be a properly cleared, disinterested party that is neither a TSCO, alternate, or subordinate to either official. The inventory will consist of a physical sighting of the material or written evidence of authorized disposition, such as certificate of destruction or receipt of transfer. At the time of the inventory, each Top Secret document or material will be physically examined for completeness and the TSCO will ensure that the accountability record accurately reflects the material held. Discrepancies found during the inventory will be resolved immediately or, where they cannot be immediately resolved, referred to the command's SM for further investigation.

e. In activities that store exceptionally large volumes of Top Secret material, ACOMs, ASCCs, and DRUs can authorize the inventory of Top Secret material to be limited to documents and material to which access has been granted within the past year and 10 percent of the remaining inventory. The 10 percent will be randomly selected. ACOMs, ASCCs, and DRUs will document these authorizations and retain such documentation for as long as the authorization remains. In such cases, ACOM, ASCC, and DRU oversight will include a spot inventory of randomly selected Top Secret material during self-inspections or other security reviews.

f. Before leaving the command, the TSCO or alternate will conduct a joint inventory with the new TSCO or alternate of all Top Secret material for which they have custodial responsibility. In addition, a 100 percent inventory of all Top Secret material held by the command is advised, but not required. However, the new TSCO or alternate will be held accountable for all top secret material for which they have custodial responsibility.

g. Accountability for Top Secret SCI, SAP, and other special types of classified information will be in accordance with AR 380–28 and AR 380–381.

## **5–19. Foreign government information**

NATO classified information will be controlled and safeguarded according to USSAN Instruction 1–07. Further, NATO unclassified information may be processed on the nonclassified internet protocol router network (NIPRNET) and/or internet-connected ISSs. Other FGI will be controlled and safeguarded as provided below (see glossary for FGI definition).

a. Classified FGI will 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 are acceptable.

b. FGI will 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, a U.S. marking that results in a degree of protection equivalent to that required by the foreign government will be applied. Comparable U.S. classification designations for FGI can be found in DoDM 5200.01, Volume 2.

c. U.S. documents containing FGI will be marked as required by DoDM 5200.01, Volume 2. 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.

d. Security clearances issued by the U.S. Government are valid for access to classified FGI of a comparable level.

e. The transmission of FGI within the United States among government agencies and U.S. contractors and between U.S. contractors with a need-to-know must be in accordance with this regulation and DoD 5220.22–M.

f. 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 chapter 7, section II for further guidance on transfer of classified information.

g. The receiving agencies will protect FGI to at least a degree equivalent to that required by the foreign government or international organization that provided the information. FGI will 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.

(1) *Control of foreign government Top Secret information.* Maintain records for 5 years from 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 will be witnessed.

(2) *Control of foreign government Secret information.* Maintain records for 3 years from 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.

(3) *Control of foreign government Confidential information.* Maintain records for 2 years from 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.

(4) *Foreign government restricted information and information provided in confidence.* To ensure the protection of Restricted FGI or foreign government unclassified information provided in confidence, such information will be classified in accordance with EO 13526. If the foreign protection requirement is lower than the protection required for

U.S. Confidential information, the information will be marked “CONFIDENTIAL–Modified Handling” as described in DoDM 5200.01, Volume 2, and the following requirements will also be met:

(a) The information will be provided only to those individuals who have an established need-to-know and where access is required by official duties.

(b) Individuals given access will 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.

(c) Documents will be stored to prevent unauthorized access (for example, a locked desk or cabinet or a locked room to which access is controlled).

h. FGI will 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 Counterintelligence and Security Agency (DCSA) 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.

i. When authorized by a bilateral arrangement, Memorandum of Cooperation, or other properly executed agreement, otherwise unclassified FGI transferred to DoD’s possession may be processed on the NIPRNET or other internet-connected ISs. This authorization must be described in the governing agreement. If subject agreement is not in place, continue to protect any FGI received as “CONFIDENTIAL–Modified Handling,” in accordance with DoDM 5200.01, Volume 2.

## **5–20. Working papers**

Working papers are documents (for example, notes, drafts, prototypes) or materials (for example, printer ribbons, photographic plates), regardless of media accumulated or created in the preparation of a finished product. Working papers containing classified information will be:

- a. Dated when created.
- b. Conspicuously marked as “WORKING PAPERS” on the cover and/or the first page of the document (or comparable location for special types of media) in letters larger than the text.
- c. Marked with the highest classification of any information contained in the material.
- d. Protected in accordance with the assigned classification.
- e. Destroyed when no longer needed.
- f. Accounted for, controlled, and marked in the same manner prescribed for a finished document of the same classification when:

(1) Released by the originator outside the command or transmitted electronically or through message center channels within the activity (exclusive or through a local area network or other IS when the transmission does not go beyond the command).

(2) Retained for more than 180 days from the date of origin.

(3) Filed permanently.

## **5–21. Reproduction of Classified Material**

Documents and other material containing classified information will be reproduced only when necessary for the accomplishment of the command’s mission or for compliance with applicable statutes or directives. Reproduction equipment and the reproduction process involve substantial risk. Therefore, commands will establish and enforce procedures for the reproduction of classified material which limit reproduction to that which is mission essential and will make sure that appropriate countermeasures are taken to negate or minimize any risk. All copies of classified documents reproduced for any purpose, including those incorporated in working papers, are subject to the same safeguards and controls prescribed for the document from which the reproduction is made. Reproduced material will be clearly identified as classified at the applicable level. Waste products generated during reproduction will be properly safeguarded as appropriate to the level of classification contained within, and destroyed in a manner approved for the destruction of classified information at that classification level.

a. Stated prohibition against reproduction of information at any classification level will be prominently displayed and strictly observed (for example, notices stating “Reproduction Only by Permission of Originator”).

b. Specific equipment will be designated for the reproduction of classified information. Such equipment cannot be designated for classified reproduction if it leaves latent images in the equipment or on other material. Exceptions are that the equipment is in a secure area or other area approved for the storage of classified information, the equipment

is protected as classified material, and the material on which the image resides is destroyed as classified waste. Rules for reproduction of classified information will be posted on or near the designated equipment.

c. Personnel who operate reproduction equipment will be made aware of the risks involved with the specific equipment, the command procedures concerning the protection, control, and accountability of reproduced information as well as the destruction of classified waste products.

d. FGI will only be reproduced and will be controlled pursuant to guidance and authority granted by the originating government.

## **Section IV**

### **Disposition and Destruction of Classified Material**

#### **5–22. Policy**

a. Classified documents and other materials will be retained only if it is required for effective and efficient operation of the command or if retention is required by law or regulation. Commands with classified holdings will establish at least 1 day a year when specific attention and effort is focused on disposing of unneeded classified material (“clean-out day”).

b. Requests from contractors for retention of classified material will only be approved if they meet the same criteria and approvals and are in accordance with security requirements provided in the contract. See AR 380–49 for requirements governing contractor retention of classified material.

c. Documents which are no longer required for operational purposes will be disposed of in accordance with the provisions of the Federal Records Act (44 USC Chapters 21 and 33) as implemented by AR 25–400–2. Classified information is subject to the same retention criteria as unclassified information. Special care will be exercised in the placing of classified information in files designated under AR 25–400–2 as “permanent.”

d. Commands will review classified files designated as “permanent,” under AR 25–400–2, prior to forwarding to a Federal Records Center, where the files are maintained pending ultimate destruction or accession into the National Archives. Each classified document in the files will be reviewed to ensure:

- (1) The classified material is a necessary part of the file as described in AR 25–400–2.
  - (2) Only the record copy is placed in the file and duplicate copies are destroyed.
  - (3) The classified material has been reviewed for downgrading and declassification and is properly remarked if downgraded or declassified.
  - (4) Any legacy-marked For Official Use Only or FOUO information contained in the document will be reviewed to determine if it can be designated as CUI and, if so, remarked in accordance with DoDI 5200.48. It is recommended that unclassified documents in the file that contain CUI be checked at the same time to make sure they are properly identified on the documents, file, and SF 135 (Records Transmittal and Receipt).
  - (5) The subject of the classified information is adequately described on the file label.
  - (6) RD, FRD, and FGI are not intermingled with other information, and are clearly marked on the file and accompanying forms.
  - (7) Top Secret information is not included unless it meets the criteria stated in AR 25–400–2.
  - (8) The subject of the classified information is adequately and completely described in the accompanying documentation, the SF 135 as required by AR 25–400–2. This applies to all files, whether classified or unclassified. Classified information will not be disclosed on the SF 135; only unclassified titles may be used to identify the records.
- e. Commanders will make sure the management of the retention of classified material is included in oversight and evaluation of program effectiveness.
- f. Material which has been identified for destruction will continue to be protected as appropriate for its classification until it is destroyed.

#### **5–23. Methods and standards for destruction**

a. Classified documents and materials will be destroyed by burning or, when meeting the standards contained in chapter 3 of this regulation, by melting, chemical decomposition, pulping, pulverizing, crosscut shredding, or mutilation sufficient to preclude recognition or reconstruction of the classified information. Strip shredders will not be used to destroy classified information.

b. Systems which involve the collection of classified material for later destruction; for example, the use of burn bags to store classified information, will include provisions for minimizing the possibility of unauthorized removal and/or access while awaiting destruction. Burn bags will be safeguarded in accordance with this regulation until destroyed.

## **5–24. Records of destruction**

*a.* Records of destruction are required for Top Secret documents and material as part of the command's Top Secret control process, where applicable (see para 5–18). The record will be executed when the material is actually destroyed, or when it is torn and placed in a burn bag or similar container. Two persons will sign the destruction record as witnessing the destruction. DA Form 3964 may be used for this purpose. Destruction records are not required for waste materials (scratch notes, typewriter and printer ribbons, and carbon paper) containing Top Secret information, unless that material has been placed on an accountability record.

*b.* Records of destruction are not required for Secret or Confidential material unless required by the originator, except for NATO and foreign government documents. For guidance on requirements for NATO classified material, to include retention standards, refer to USSAN 1–07.

## **Chapter 6 Storage and Physical Security Standards**

### **Section I**

#### **General**

### **6–1. Policy**

Classified information will be secured under conditions adequate to prevent access by unauthorized persons and meet the minimum standards specified in this regulation. An assessment of the threat to the material, the location of the command, and the sensitivity of the information will be considered when determining if the minimum requirements of this chapter require enhancement, as determined by the local command.

### **6–2. Physical security policy**

*a.* Physical security is intended to be built upon a system of defense, or security-in-depth as defined in the glossary, to provide accumulated delay time. AR 190–13 provides additional information on the principles of physical security.

*b.* AR 190–13 prescribes minimum uniform standards and procedures in the use of security identification cards and badges to control personnel movement into and within restricted areas.

### **Section II**

#### **Storage Standards**

### **6–3. Standards for storage equipment**

*a.* GSA establishes and publishes minimum standards, specifications, and supply schedules for approved security containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.

*b.* The DoD Lock Program is the technical authority for securing a storage facility and containers with approved locking devices for the protection of classified information. For technical assistance concerning classified material storage standards, commands can contact the DoD Lock Program Technical Support Hotline. Contact information is available at <https://navfac.navy.mil>.

### **6–4. Storage of classified information**

*a.* Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked security container, vault, room, or area pursuant to the level of classification and this regulation by one or more of the following methods:

(1) Top Secret information will be stored as identified below:

(*a*) In a GSA-approved security container with one of the following supplementary controls: an employee cleared to at least the Secret level will inspect the security container once every 2 hours, but not in a way that indicates a pattern, or the location that houses the security container is protected by an intrusion detection system (IDS) meeting the requirements of section III of this chapter, with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(*b*) In a GSA-approved container equipped with a lock meeting Federal Specification FF–L–2740, provided the container is located within an area that has been determined to have security-in-depth.

(c) In an open storage area (also called a secure room) constructed in accordance with section III of this chapter and equipped with an IDS with the personnel responding to the alarm arriving 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.

(d) In a vault, or GSA-approved modular vault, meeting the requirements of FED-STD 832 as specified in section III of this chapter.

(e) Under field conditions during military operations, commanders can prescribe measures deemed adequate to meet the storage standard contained in paragraph 6-4b(1).

(2) Secret information will be stored by one of the following methods:

(a) In the same manner as prescribed for Top Secret information,

(b) In a GSA-approved security container or modular vault or vault built to FED-STD 832 without supplementary controls, or

(c) In an open storage area meeting the requirements of this regulation, provided that security-in-depth exists and one of the following supplemental controls is used: an employee cleared to at least the Secret level will inspect the open storage area once every 4 hours, or an IDS meeting the requirements of section III of this chapter with the personnel responding to the alarm arriving within 30 minutes of alarm annunciation.

(3) Confidential information will be stored in the same manner as prescribed for Top Secret or Secret information except that supplementary controls are not required.

b. Specialized security equipment.

(1) GSA-approved field safes and special purpose one- and two-drawer lightweight security containers approved by the GSA are used primarily for storage of classified information in the field and in military platforms, and will be used only for those or similar purposes. These containers will use locks conforming to Federal Specification FF-L-2740 or FF-L-2937 as required by Federal Specification AA-F-358. Special size containers will be securely fastened to the platform; field safes will be under sufficient control and surveillance when in use to prevent unauthorized access or loss.

(2) GSA-approved map and plan files are available for storage of odd-sized items such as computer media, maps, charts, and classified equipment.

(3) GSA-approved modular vaults, meeting Federal Specification AA-V-2737, can be used to store classified information as an alternative to vault requirements described in section III of this chapter.

c. Storage areas for bulky material containing Secret or Confidential information may have access openings (for example, roof hatches, vents) secured by GSA-approved, changeable combination padlocks meeting Federal Specification FF-P-110. Other security measures are required in accordance with paragraph 6-4a(2) and 6-4a(3).

(1) When special circumstances exist, key operated locks may be used for storage of bulky material containing Secret and Confidential information. It will be the responsibility of the command to document this requirement outlining the special circumstances that warrant deviation from the changeable combination padlock standard in paragraph 6-4c and establish administrative security standard operating procedures for the control and accountability of keys and locks whenever key operated, high security padlocks are utilized. At a minimum, the following procedures will be implemented:

(a) A key and lock custodian will be appointed and cleared at the Secret level in writing to ensure proper custody and handling of keys and locks.

(b) A key and lock control register will be maintained to identify keys, the number of keys for each lock, and the current location and custody.

(c) Keys will be inventoried with each change of custodian. Keys will not be removed from the premises.

(d) Keys that are not issued to users on hand receipt and spare locks will be stored in a GSA-approved security container or other secure container that meets Federal Specification FF-L-2740.

(e) To reduce the risk of a padlock being swapped while the container is opened, the padlock and the key will be either placed in the security container or the padlock will be locked to the hasp and the key either be personally retained, stored in a central location, or placed inside the unlocked container.

(f) Key operated locks will be changed or rotated at a minimum of once every 2 years and will be immediately replaced upon loss or compromise of their keys.

(2) 18 USC Section 1386 makes unauthorized possession of keys, key-blanks, key-ways or locks adopted by any part of the DoD for use in the protection of conventional arms, ammunition, explosives, special weapons, or classified information or equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.



#### **6-5. Procurement of new storage equipment**

New security storage equipment will 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 SM will record the lock serial number on an SF 700.

#### **6-6. Removal of classified information for work at home**

Only in extreme mission critical and exceptional situations will classified information be authorized for storage in an individual's personal residence, on or off a military installation, or stored in any location outside a government or cleared contractor facility. If it becomes mission critical for individuals to remove classified information and materials (for example, IT equipment and associated storage media) for work at home, specific security measures and approvals are required, and security measures appropriate for the level of classification must be in place and monitored closely to provide adequate protection, security-in-depth, and to prevent access by unauthorized persons.

*a. Top Secret.* Only the SECARMY may authorize the removal of Top Secret information from designated working areas for work at home. SECARMY may also authorize removal of information for work at home for any lower level of classification.

*b. Secret and Confidential.* Commanders of ACOMs, ASCCs, DRUs, or the AASA, may authorize removal of Secret and Confidential information from designated working areas for work at home. This authority will not be further delegated.

*c. Residential storage equipment.* A GSA-approved security container will be furnished for residential storage of classified information and protected with an IDS. Other methods of supplemental control can be used in place of the IDS where other methods provide substantially the same assurance of protection. Written security procedures will be developed to provide for the appropriate protection level of the classified information and material in accordance with this regulation, including a record of the classified information and material that has been authorized for removal for work at home.

*d. Classified information technology systems.* All classified network connections (for example, SIPRNET) approved for residential use must be certified and accredited in accordance with AR 25-2.

*e. Secure terminal equipment.* In certain situations requiring immediate contact and discussion of classified information, in accordance with paragraphs 6-6a and 6-6b, the installation of a secure telephone unit (such as an STE) can be authorized in personal residences. This will not be authorized for personal convenience. Where such units are permitted, care must be exercised in ensuring that unauthorized personnel, to include family members, are not within hearing distance when classified discussions take place and that the control key for the unit is either personally retained or stored in a discreet location separate from the unit. In such cases, it can be necessary for the custodian of the unit to make notes regarding the classified discussion that occurs over the security telephone. When this occurs, such classified notes can be retained in the personal residence only until the next duty day. If the next duty day is more than 1 day or falls during a period of leave, temporary duty or other absence, the material will be delivered for storage to a government or cleared contractor facility prior to such absence. While in a personal residence, such classified notes will be safeguarded and under the personal, physical control of the authorized, cleared holder of the notes at all times.

*f. Other requirements.* In addition to the above, the following security criteria must be included in the written procedures:

(1) Storage of any level of classified information will require the material to be under the personal control of the authorized individual at all times when it is not secured in a GSA-approved security container.

(2) Employee training on classified ISs operation, as well as protection and storage of classified information and COMSEC materials.

(3) Provisions for secure storage and/or destruction of any classified information that may be required or generated (for example, storage of COMSEC key materials, classified hard drives, and documents).

(4) Application of and compliance with requirements for security-in-depth.

#### **6-7. Safeguarding of U.S. classified information located in foreign countries**

Except for classified information released to a foreign government or international organization, and under the safeguarding of that country or organization, U.S. classified material will only be retained in foreign countries when necessary to satisfy specific U.S. Government requirements. Commanders will take into consideration the additional risk associated with storing, discussing, and processing classified information outside the United States when establishing procedures to implement this regulation. Particular attention will be paid to the foreign release requirements of AR 380-10, making sure that classified material is not accessed by foreign personnel not authorized access to the information. U.S. classified material in foreign countries will be stored in accordance with DoDM 5200.01, Volume 3.

## **6–8. Equipment designations and combinations**

a. There will be no external mark revealing the level of classified information authorized to be stored in a given container, secure area, or vault. Priorities for emergency evacuation and destruction will not be marked or posted on the exterior of storage containers, vaults, or secure rooms. For identification and/or inventory purposes, each secured area, vault, or container will bear, externally, an assigned number or symbol not relating to any known security markings. This, along with the SF 702 and the “OPEN–SECURED” signs, are the only items permitted on the exterior of the security container. The top of the security container will not be used as a bookshelf or paper storage area.

b. Weapons or items such as funds, jewels, precious metals, or drugs will not be stored in the same container used to safeguard classified information.

c. Combinations to security containers, vaults, and secure rooms will be changed only by individuals who are assigned that responsibility in writing (for example, SM) and possess the appropriate security clearance. Combinations will be changed:

- (1) When placed in service.
- (2) Whenever an individual knowing the combination no longer requires access unless other sufficient controls exist to prevent that individual’s access to the lock.
- (3) When the combination has been subject to possible compromise.
- (4) When taken out of service, built-in combination locks will be reset to the standard combination 50–25–50; combination padlocks will be reset to the standard combination 10–20–30.

d. A record will be maintained for each vault, secure room, or container used for storing classified information, showing location of the container, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. SF 700 will be used for this purpose. A current record for all security containers, vault doors, and padlock combinations will be kept on SF 700.

(1) Complete part 1 and part 2A, SF 700. Include the name, date, and signature of the person making the combination change in item 9, part 1. Part 1 of SF 700 is not classified but contains personally identifiable information that will 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 on the inside of the lock drawer (or door) of the security container. If the information must be accessed during nonduty 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.

(2) Parts 2 and 2A, SF 700 will be marked with the highest classification of material stored in the container. Part 2A will then be detached and placed in the Part 2 envelope and sealed. The classification authority block will then be applied to the envelope, which will be treated as a derivative classification of that information. For example, the classification authority block on Part 2 will state “Classified By: [name of person filling out the SF 700],” Derived From: “Multiple Sources,” Declassify On: “Change of Combination.”

e. The combination of a container, vault, or secure room used for the storage of classified information will be treated as information having a classification equal to the highest classification level of the classified information to be stored inside. Such written records are classified and will be stored in containers approved for the storage of classified information, at the appropriate classification level, and stored in a security container other than the one for which it is being used. Written records of combinations will not be stored in unapproved locations, such as in wallets, purses, briefcases, desk drawers, calendars or note pads, or written “in code” or foreign languages.

f. Access to the combination of a vault, secure room, or container used for the storage of classified information will be granted only to those individuals who are authorized access to the classified information that is to be stored inside.

g. Entrances to secure rooms or areas will be either under visual control at all times during duty hours, to preclude entry by unauthorized personnel, or the entry will be equipped with electric, mechanical, or electro-mechanical access control devices to limit access during duty hours. Section III of this chapter provides standards for these access control devices. Electronically actuated locks (for example, cipher and magnetic strip card locks) and other such locking devices used primarily for duty hours access control do not afford by themselves the required degree of protection for classified information and must not be used at unattended classified areas either during or after duty hours as a substitute for the locks prescribed in paragraph 6–4b.

## **6–9. Neutralization and repair of Government Services Agency-approved security containers and vault doors**

a. Neutralization and repair of a security container or door to a vault approved for storage of classified information will be accomplished only by appropriately cleared or continuously escorted U.S. personnel specifically trained in the methods specified by reference FED–STD 809.

*b.* Neutralization or repair by, or using, methods and procedures other than described in FED–STD 809 is considered a violation of the security container’s or vault door’s security integrity and the GSA label will be removed. Thereafter, the containers or doors may not be used to protect classified information until repaired per FED–STD 809, inspected by a qualified inspector, and certified for use in writing.

#### **6–10. Maintenance and operating inspections**

Commanders of ACOMs, ASCC, and DRUs will establish procedures concerning repair and maintenance of classified material security containers, vaults, and secure rooms to include a schedule for periodic maintenance. The following guidelines pertain to spotting repair and maintenance problems that will be addressed outside the regular maintenance schedule.

*a.* Security containers are usually serviceable for at least 25 years, if properly maintained. The life span of the container is often cut short by lock or locking bolt linkage malfunctions that require neutralization of the container. Most of these problems can be detected in their early stages, and definite symptoms can warn of a developing problem. Users should be alert for these symptoms, and if any of them are detected, the users should immediately contact their supporting SM. It is important to never use force to try to correct the problem. Critically needed material should not be stored in containers showing any of these symptoms, since they cannot be depended upon to open again. Should that occur, the user can be faced with a lockout.

*b.* Users should watch for the following signs of trouble:

- (1) A dial that is unusually loose or difficult to turn.
- (2) Any jiggling movement in the dial ring. This is often detected when a twist motion is applied to the dial.
- (3) Difficulty in dialing the combination or opening the container.
- (4) Difficulty with the control drawer or other drawers. Examples are as follows:

*(a)* Drawers rubbing against container walls. This can be caused if the container is not leveled, or the tracks or cradles are not properly aligned.

*(b)* Problems with opening or closing drawers because the tracks or cradles need lubricant, material is jammed in behind the drawer, or the internal locking mechanism is tripped.

(5) Difficulty in locking the control drawer. Examples are as follows:

- (a)* The control drawer handle or latch will not return to the locking position when the drawer is shut.
- (b)* The locking bolts move roughly, slip, or drag, or the linkage is burred or deformed.

(6) GSA approval labels are missing or in need of replacement. If missing, contact the DoD lock program to obtain information on retaining an authorized inspector. GSA-approved security containers and vault doors must have a GSA approval label or a GSA recertification label on the front of the equipment in order to store classified information.

*c.* Commanders will periodically remind users of containers about the above guidelines.

#### **6–11. Turn-in or transfer of security equipment**

In addition to having combinations reset before turn-in (see para 6–8c(4)), security equipment will be inspected before turn-in or transfer to ensure that classified material is not left in the container. The turn-in procedure will include removal of each container drawer and inspection of the interior to make sure that all papers and other material are removed and that the container is empty. Incinerators, shredders, or other classified material destruction devices, as well as the rooms in which they are located, will be thoroughly inspected to make sure that no classified material remains. A written, signed record certifying that this inspection has been accomplished and that no classified material remains will be furnished to the SM and filed for 2 years in accordance with AR 25–400–2.

### **Section III**

#### **Physical Security Standards**

#### **6–12. General**

This section provides the general construction standards for areas approved for the open storage of classified information, general standards for intrusion detection (alarm) systems (IDS) used in areas in which classified information is stored, and access control standards. Classified material will be stored in GSA-approved security containers. Open storage areas will only be approved when storage in other approved security containers is not feasible due to the size, shape, or volume of material stored.

#### **6–13. Vault and secure room (open storage area) construction standards**

*a.* Vaults will meet the construction standards outlined in FED–STD 832, as follows:

- (1) Class A (concrete poured-in-place).
- (2) Class B (GSA-approved modular vault meeting Federal Specification AA-V-2737).
- (3) Class C (steel-lined vault) is not authorized for protection of classified information.
- b. Secure room (open storage area). Below are the minimum construction standards for open storage areas:
  - (1) *Walls, floor, roof.* Walls, floor, and roof must be of permanent construction materials; for example, plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to and evidence of unauthorized entry into the area. Walls will 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 will be constructed of plaster, gypsum, wallboard material, hardware, or other similar material to be of equivalent strength.
  - (3) *Doors.* Access doors will be substantially constructed of wood or metal. For out-swing doors, hinge-side protection will be provided by making hinge pins nonremovable (for example, spot welding) or by using hinges with interlocking leaves that prevent removal. Doors will be equipped with a GSA-approved combination lock meeting FF-L-2740. Doors other than those secured with locks meeting FF-L-2740 will 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.* 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, will 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 military installation or 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). Windows, which might reasonably afford visual observation of classified activities within the facility, will be made opaque or equipped with blinds, drapes, or other coverings.
  - (5) *Openings.* Utility openings such as ducts and vents will 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 will be hardened in accordance with MIL-HDBK 1013/1A.

#### **6-14. Intrusion detection system standards**

- a. An IDS, often referred to as an alarm, must detect an unauthorized penetration in the secured area. An IDS will be installed when results of a documented risk assessment to determine its use as a supplemental control is warranted, in accordance with this regulation, and use is approved by commanders of ACOMs, ASCCs, or DRUs or AASA. When used, all areas that reasonably afford access to the security container or areas where classified data is stored will be protected by an IDS unless continually occupied. An IDS complements other physical security measures and consists of the following:
  - (1) IDS or intrusion detection equipment (IDE).
  - (2) Security forces.
  - (3) Operating procedures.
- b. System functions. IDS components operate as a system with the following four distinct phases:
  - (1) Detection.
  - (2) Communications.
  - (3) Assessment.
  - (4) Response.
- c. These elements are equally important. None can be eliminated if the IDS is to provide an acceptable degree of protection.
  - (1) *Detection.* The detection phase begins as soon as a detector or sensor reacts to 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. This will be used as the definition of an alarmed zone for purposes of this regulation.
  - (2) *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 (for example, 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.

(3) *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.

(4) *Response.* The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response phase must also determine the precise nature of the alarm and take all measures necessary to safeguard the secure area.

## **6–15. Selection of equipment**

*a. General.* As determined by the commander, and in accordance with this regulation, all areas that reasonably afford access to the container or facility, or where classified data is stored, are to be protected by IDS unless continually occupied. Prior to the installation of an IDS, commanders, or their designated personnel, will consider the threat, vulnerabilities, and any in-depth security measures and will perform a risk analysis to determine if an IDS is appropriate to the situation.

*b. Acceptability of equipment.* All IDE must be Underwriters Laboratories (UL)-listed, or equivalent, and approved by the DA or authorized government contractor. Government installed, maintained, or furnished systems are acceptable.

## **6–16. Intrusion detection system transmission and annunciation**

*a. Transmission line security.* When the transmission line leaves the facility and traverses an uncontrolled area, Class I or Class II line supervision will be used.

(1) *Class I.* Class I line security is achieved using National Institute of Standards and Technology-approved implementation of the Advanced Encryption Standard.

(2) *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 will not repeat itself within a minimum 6-month period. Class II security will be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

*b. Internal cabling.* The cabling between the sensors and the PCU must be dedicated to the IDE and must comply with national and local code standards.

*c. Entry 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 must be subordinate in priority to reports from intrusion alarms.

*d. Maintenance mode.* When the alarm zone is placed in the maintenance mode, this condition will be signaled automatically to the monitor station. The signal must appear as an alarm or maintenance message at the monitor station and the IDS will not be securable while in the maintenance mode. The alarm or message must be continually visible at the monitor station throughout the period of maintenance. A standard operating procedure will be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods will be archived in the system. A self-test feature will be limited to 1 second per occurrence. The maintenance program for the IDS should ensure that incidents of false alarms be investigated and should not exceed one in a period of 30 days per zone.

*e. Annunciation of shunting or masking condition.* Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.

*f. Indications.* Indications of alarm status will be revealed at the monitoring station and optionally within the confines of the secure area.

*g. Power supplies.* Primary power for all IDE will be commercial alternating current (AC) or direct current (DC) power. In the event of commercial power failure at the protected area or monitor station, the equipment will change power sources without causing an alarm indication.

(1) *Emergency power.* Emergency power will consist of a protected independent backup power source that provides a minimum of 8 hours of operating power via battery and/or generator power. When batteries are used for emergency power, they will be maintained at full charge by automatic charging circuits. The manufacturer's periodic maintenance schedule will be followed and results documented.

(2) *Power source and failure indication.* An illuminated indication will exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station will indicate a failure in power source, a change in power source, and the location of the failure or change.

*h. Component tamper protection.* IDE components located inside or outside the secure area will be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection will be provided.

## **6–17. System requirements**

*a. Independent equipment.* When many alarmed areas are protected by one monitor station, secure room zones and areas in which classified information is stored must be clearly distinguishable from the other zones to ensure a priority response. All sensors will be installed within the protected area.

*b. Access and/or secure switch and premise control unit.* No capability is to exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs must be located inside the secure area and are to be located near the entrance. Only assigned personnel will initiate changes in access and secure status. Operation of the PCU can be restricted by the use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space will cause an alarm to be transmitted to the monitor station.

*c. Motion detection protection.* Secure areas that reasonably afford access to the security container or where classified data is stored are to be protected with motion detection sensors, for example, 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 will cause an immediate and continuous alarm condition.

*d. Protection of perimeter doors.* Each perimeter door will be protected by a Balanced Magnetic Switch that meets the standards of UL 634.

*e. Windows.* All readily accessible windows (within 18 feet of ground level) will be protected by an IDS, either independently or by the motion detection sensors in the space, whenever a secure room is located within a controlled compound or equivalent and forced entry protection of the windows is not provided (see para 6–13b(4)).

*f. Intrusion detection system requirements for continuous operations facilities.* A continuous operations 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 could also be required depending upon the situation.

*g. 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 will be investigated and the results documented. The maintenance program for the IDS must ensure that incidents of false and/or nuisance alarms do not exceed one in a period of 30 days per zone.

## **6–18. Installation, maintenance, and monitoring**

*a. Intrusion detection system installation and maintenance personnel.* Alarm installation and maintenance will be accomplished by U.S. citizens who have been subjected to a trustworthiness determination in accordance with AR 380–67.

*b. Monitor station staffing.* The monitor station is to be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination in accordance with AR 380–67.

*c. Periodic functionality checks.* Security personnel will perform a function-test of all installed IDS sensors, at a minimum, semi-annually. Nonfunctioning sensors will be documented and repaired or replaced as soon as possible. Pending sensor repair or replacement, the SM will reassess measures for security-in-depth or other supplemental security controls and augment them as may be required to ensure adequate protections for classified material.

## **6–19. Access controls while material is not secured in security containers**

This section applies to open storage areas such as vaults and secure rooms. It can also apply at the ACOM, ASCC, or DRU option to other areas of security interest, such as areas in which significant amounts of classified material or especially sensitive material are routinely accessed. This section does not apply to open storage of SAP material. See AR 380–381 regarding open storage of SAP material and information.

*a.* The perimeter entrance to a secure area (for example, vault or secure room) will be under visual control at all times during working hours to prevent entry by unauthorized personnel. This can be accomplished by several methods, such as an employee work station, guard, or closed-circuit television. Regardless of the method used, an access control system will be used on the entrance.

*Note.* Uncleared persons will be escorted within the facility by a cleared person who is familiar with the security procedures at the facility, and an announcement, either auditory or visual, will be used to alert others of the uncleared person's presence.

b. An Automated Entry Control System (AECS) can be used to control admittance during working hours instead of visual or other methods of control. AECS must identify an individual and authenticate the person's authority to enter the area using one of the following:

(1) *Identification badges or key cards.* The identification badge or key card must 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.

(2) *Personal identity verification.* Biometrics verification can be used to verify an individual's access to classified information, CUI, or IT systems.

*Note.* A biometrics device can be particularly appropriate for access to areas in which highly sensitive information is located. The Defense Forensics and Biometrics Agency (<https://www.dfba.mil/>) can provide further information regarding biometric technologies and capabilities.

c. In conjunction with paragraph 6–19b(1), a personal identification number (PIN) can be required. The PIN must be separately entered into the system by each individual using a keypad device and will consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN must be changed or discontinued when it is believed to have been compromised, subjected to compromise, or the individual no longer requires access.

d. Authentication of the individual's authorization to enter the area must be accomplished within the system by inputs from the identification badge and/or card, the personal identity verification device, or the keypad with an electronic database of individuals authorized to enter the area. Procedures will be established, in writing, for removal of 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.

e. Protection must be established and maintained for all devices or equipment which constitutes the entry control system. The level of protection can vary depending upon the type of device or equipment being protected. This can be accomplished by the following:

(1) Location where authorization data and personal identification or verification data is entered or inputted, stored, or recorded, is protected.

(2) Card readers, keypads, communication, or interface devices located outside the entrance to a controlled area will have tamper resistant enclosures and be securely fastened to the wall or other permanent structure. Control panels located within a controlled area will require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.

(3) Keypad devices will be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.

(4) Systems that use transmission lines to carry access authorizations, personal identification data, or verification data between devices or equipment located outside the controlled area will have line supervision (see para 6–16 for explanation of line supervision).

(5) Electric strikes used in access control systems will be heavy duty, industrial grade.

f. Records will be maintained reflecting active assignment of identification badge/card, PIN, level of access, and similar system-related records. Records concerning personnel removed from the system will be retained for 90 days. Records of entries will be retained for at least 90 days or until any investigations of system violations and incidents have been investigated, resolved, and recorded. Refer to AR 25–400–2 for records disposition and destruction requirements.

(1) Access to records and information concerning encoded identification data and PINs will be restricted. Access to identification or authorizing data, operating system software, or any identifying data associated with the entry control system will be limited to the fewest number of personnel as possible.

(2) Such data or software will be kept secure when unattended. Personal information will be purged or cleared from AECSs (to include purging from Biometric-like technology) when the individual no longer requires access and as stated in paragraph 6–19f.

g. Personnel who are the first to enter or last to leave an area will be required to secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirmation of security clearance, need-to-know, and access. Commanders can approve the use of standardized AECS which meet the criteria below:

(1) For a Level 1 key card system, for example, a key card bearing a magnetic stripe, the AECS will provide .95 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 a probability of less than .05 after three attempts to gain entry.

(2) For a Level 2 key card and PIN system, for example, a key card bearing a magnetic stripe used in conjunction with a PIN and biometrics identifier system, the AECS will provide a .97 probability of granting access to an authorized user providing the proper identifying information within three attempts have been made. In addition, the system must ensure an unauthorized user is granted access with a probability of less than .010 after probability after three attempts to gain entry have been made.

(3) For a Level 3 key card and PIN and biometrics identifier system, the AECS must provide a .97 probability of granting access to an authorized user providing the proper identifying information within three attempts. In addition, the system must ensure an authorized user is granted access with a probability of less than .005 after three attempts to gain entry have been made.

*h.* Electric, mechanical, or electromechanical devices that meet the criteria stated below may be used to control admittance to secure areas during duty hours, if the entrance is under visual or other command approved system of control by cleared authorized personnel located in the area. These devices are also acceptable to control access to selected or otherwise compartmented areas within a secure area. Nothing in this statement is intended to modify the policy stated in AR 380–28. Access control devices will be installed in the following manner:

(1) The electronic control panel containing the mechanism by which the combination is set must be located inside the area. The control panel, located within the area, will require only minimal degree of physical security designed to preclude unauthorized access to the mechanism.

(2) The control panel will be installed in such a manner, 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) The selection and setting of the combination will be accomplished by an individual cleared at the same level as the highest classified information controlled within.

(4) Electrical components, wiring included, or mechanical links (cables, rods, and so on) should be accessible only from inside the area, or, if they traverse an uncontrolled area, they should be secured within protecting covering to preclude surreptitious manipulation of components.

## **Chapter 7**

### **Transmission and Transportation**

#### **Section I**

#### **Methods of Transmission or Transportation**

##### **7–1. Policy**

Classified information will be transmitted or transported as specified in this chapter. Commands will establish local procedures to meet the requirements to minimize risk of compromise while permitting use of the most cost effective transmission or transportation means. External, street side collection boxes (for instance U.S. mailboxes) will not be used for the dispatch of classified information. Commands will develop procedures to protect incoming mail, bulk shipments, and items delivered by messenger, until a determination is made whether classified information is contained therein. Screening points will be established to limit access to classified information to only cleared personnel.

*a.* COMSEC material will be transmitted and transported according to AR 380–40.

*b.* NATO classified information, including NATO restricted, will be transmitted and transported according to the requirements outlined in USSAN 1–07.

##### **7–2. Dissemination outside the Department of Defense**

*a.* Classified information originating in another agency within the DoD or in another department or agency outside the DoD may be disseminated to other DoD agencies, other United States departments or agencies, or a U.S. entity without the consent of the originating DoD component, department, or agency, as long as:

(1) The criteria for access to classified information outlined in chapter 3 are met.

(2) The classified information is not marked as requiring authorization for dissemination to another department or agency. The originator's controlled marking may be used to identify information requiring prior authorization for dissemination to another department or agency.

(3) The document was created on or after 25 June 2010, the effective date of 32 CFR 2001. Documents created before 25 June 2010 may not be disseminated outside of the DoD without the originator's consent. Additionally, documents created on or after 25 June 2010, whose classification is derived from documents created prior to that date, and where the date before 25 June 2010 of the classified source(s) is readily apparent from the source list, will not be disseminated outside the DoD without the originator's consent.



- b.* Classified information originating in, or provided to or by the DoD may be disseminated to a foreign government or an international organization of governments, or any element thereof, in accordance with AR 380–10.
- c.* Dissemination of information regarding intelligence sources, methods, or activities will be consistent with directives issued by the DNI and in accordance with AR 380–28.
- d.* Dissemination of classified information to state, local, tribal, and private sector officials pursuant to EO 13549 will be in accordance with the implementing guidance issued by the Department of Homeland Security.

### **7–3. Top Secret information**

Top Secret information will be transmitted and transported only by:

- a.* Direct contact between appropriately cleared persons.
- b.* Electronic means over an approved secure communications system. This applies to voice, data, message, and facsimile transmissions (see AR 25–2).
- c.* The Defense Courier Division (DCD) if the material qualifies under the provisions of DoDI 5200.33. The DCD may use a specialized shipping container as a substitute for a DCD courier on direct flights if the shipping container is sufficiently constructed to provide evidence of forced entry, secured with a high security padlock meeting FF–P–110 specifications and equipped with an electronic seal that would provide evidence of surreptitious entry. A DCD courier must escort the specialized shipping container to and from the aircraft and oversee its loading and unloading. This authorization also requires that the DCD develop procedures that address protecting specialized shipping containers if a flight is diverted for any reason.
- d.* Authorized command courier or messenger services.
- e.* The Department of State Diplomatic Courier Service.
- f.* Appropriately cleared U.S. military and U.S. Government civilian personnel specifically designated to carry the information and traveling by surface transportation or traveling on scheduled commercial passenger aircraft within and between the United States, its territories, and Canada.
- g.* Appropriately cleared U.S. military and U.S. 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 the appropriate clearances traveling within and between the United States and its territories when the transmission has been authorized, in writing, by the appropriate cognizant security agency or a designated representative (see AR 380–49).

### **7–4. Secret information**

Secret information can be transmitted and transported by:

- a.* Any of the means approved for the transmission of Top Secret information.
- b.* United States Postal Service (USPS) registered mail within and between the United States, the District of Columbia, and the Commonwealth of Puerto Rico.
- c.* USPS Priority Mail Express (formerly referred to as Express Mail) within and between the United States, the District of Columbia, and the Commonwealth of Puerto Rico. The “Waiver of Signature and Indemnity” block on the USPS Label 11–B (Priority Mail Express) may not be executed under any circumstances. The use of external (street side) Express Mail collection boxes is prohibited.
- d.* USPS and Canadian registered mail with registered mail receipt between U.S. Government and Canadian government installations in the U.S. and Canada.
- e.* USPS 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.
- f.* As an exception, in urgent situations requiring next-day delivery within the United States and its territories, commanders may 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 in accordance with chapter I of Title 39, CFR are met. Any such delivery service will be U.S. owned and operated, provide automated in-transit tracking of the classified information, and ensure package integrity during transit. The contract will 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 email) that the package did in fact arrive within the specified time. The package may be addressed to the recipient by name. The release signature block on the receipt label will not be executed under any circumstances. The use of external (street side) collection boxes is prohibited. Classified COMSEC, NATO information, SCI, and FGI will not be transmitted in this manner. See Multiple Award

Schedule 48 (Transportation, Delivery, and Relocation Solutions) on the GSA eLibrary website at <https://www.gsaelibrary.gsa.gov/> for a listing of commercial carriers authorized for use under the provisions of this paragraph.

*Note.* In many situations, the USPS Priority Mail Express can meet the next-day delivery standards and should be used, as noted in paragraph 7–4c.

g. Carriers cleared under the National Industrial Security Program providing a protective security service. This method is authorized only within the continental United States 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.

h. Appropriately cleared contractor employees, provided that the transmission meets the requirements specified in DoDM 5220.22, Volume 2 and DoD 5220.22–M.

i. U.S. Government and U.S. Government contract vehicles, including aircraft, ships of the U.S. Navy, civil service-operated U.S. Navy 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 that control of the carrier is maintained on a 24-hour basis. The escort will protect the shipment at all times, through personal observation or authorized storage, to prevent inspection, tampering, pilferage, or unauthorized access. Observation of 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. The escort will, if possible, observe the loading of the shipment.

## **7–5. Confidential information**

Confidential information may be transmitted and transported by:

- a. Any means approved for the transmission of Secret information.
- b. USPS registered mail will be used for Confidential material only as indicated below:
  - (1) Material to and from military post office addressees (for example, Army Post Office or Fleet 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. USPS certified mail (or registered mail, if required above) for material addressed to DoD contractors or non-DoD agencies.
- d. USPS first class mail between DoD Component locations anywhere in the United States and its territories. The outer envelope or wrapper will be endorsed: “Return Service Requested.”
- e. Commercial carriers that provide Constant Surveillance Service, as defined by DoD 5220.22–M, within and between the 48 contiguous states and the District of Columbia or wholly within Alaska, Hawaii, or a U.S. territory.
- 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 government control. The commanders or masters will 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 will not be unloaded.
  - (2) Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

## **Section II**

### **Transmission and Transportation of Classified Material**

#### **7–6. Transmission and transportation of classified material to foreign governments**

Classified information or material approved for release to a foreign government or international organization, in accordance with AR 380–10, will be transferred between representatives of each government through government-to-government channels or through other channels agreed to in writing by the designated authorities of the sending and receiving governments.

a. For foreign government or international organization transfers of classified material, DA commands will follow guidance outlined below and within the appendix to DoDM 5200.01, Volume 3, Enclosure 4.

(1) U.S. Government control and accountability of classified information or material will 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.

(2) In urgent situations, appropriately cleared U.S. Government agency employees may be authorized to hand-carry classified material in accordance with this chapter and DoDM 5200.01, Volume 3, Enclosure 4.

b. Each DA command entering into a contract or an international agreement that will involve the transfer of classified information and material to a foreign government will consult with supporting DoD transportation and security authorities to confirm the appropriate transfer arrangements and establish responsibilities for the transfer arrangements prior to any execution of the agreement or contract. Transportation plan requirements are outlined in DoDM 5200.01, Volume 3, Enclosure 4.

### **7-7. Preparation of material for shipment by freight**

Where applicable, commands will establish procedures for shipment of bulk classified material as freight, to include provisions for shipment in closed vehicles, when required, appropriate notice to the consignee concerning the shipment, procedures at transshipment activities, and action to be taken in case of nondelivery or unexpected delay in delivery.

### **7-8. Envelopes or containers**

a. When transferring classified information, it will be enclosed in two opaque, sealed envelopes, wrappings, or lockable containers durable enough to properly protect the material from accidental exposure and to ease in detecting tampering. The following exceptions apply:

(1) If the classified material is an accessible internal component of an item of equipment, the outside shell or body can be considered as the inner enclosure provided it does not reveal classified information.

(2) If the classified material is an inaccessible internal component of a bulky item of equipment, the outside or body of the item can be considered to be a sufficient enclosure provided observation of it does not reveal classified information.

(3) If the classified material is an item or piece of equipment that cannot be packaged and the shell or body is classified, it will be concealed with an opaque covering that will hide all classified features.

(4) Specialized shipping containers, including closed cargo transporters, can be considered the outer wrapping or cover when used.

b. When classified material is hand-carried outside an activity, a locked briefcase or zippered pouch made of canvas or other heavy duty material and having an integral key operated lock can serve as the outer wrapper. In other cases, these items may 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 will be left for subsequent opening by the intended recipient, package the material as required by paragraph 7-8a and additionally observe the following procedures:

(1) 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.

(2) Serially number the pouch or briefcase and clearly display this serial number on its exterior surface.

(3) Lock the briefcase or pouch and place its key in a separate sealed envelope and store the briefcase or pouch, when containing classified material, according to the highest classification level and any special controls applicable to its contents.

(4) 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.

(5) Use a briefcase or pouch only to assist in enforcing need-to-know. Its use will in no way alleviate the individual's 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.

c. Classified material will be prepared for shipment, packaged, and sealed in ways that minimize the risk of accidental exposure or undetected deliberate compromise. Documents will be packaged so that the classified text is not in direct contact with the inner envelope or container.

d. For documents that do not have an unclassified cover or cover transmittal letter or form, this can be accomplished by inserting an opaque sheet or cardboard sheet on top of the classified text in the inner envelope.

### **7-9. Addressing**

a. The outer envelope or container for classified material will be addressed to an official U.S. Government activity or to a DoD contractor with a facility clearance and appropriate storage capability. It will show the complete return address of the sender. The outer envelope will not be addressed to an individual. Office codes or phrases such as "Attention: Research Department" may be used.

b. The inner envelope or container will 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, and any other special instructions. The inner envelope may have an “attention line” with a person’s name.

c. The outer envelope or single container will not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified.

d. Classified information intended only for U.S. elements of international staffs or other organizations must be addressed specifically to those elements.

#### **7–10. Mail channels with other government agencies**

Other federal government agencies can require special certification or special procedures before forwarding classified information to another agency. When that is the case, DA commands will comply with the requirements of those agencies.

### **Section III**

#### **Escort or Hand-Carrying of Classified Material**

##### **7–11. General provisions**

a. Appropriately cleared and briefed DA personnel may be authorized to escort or hand-carry classified material between locations when other approved means of transmission or transportation cannot be used. Hand-carrying of classified material will be limited to situations of absolute necessity and will be carried out to make sure it does not pose an unacceptable risk to the information. Generally, two-way hand-carrying, for example carrying the material both to and from the destination, is not authorized unless specific justification has been provided and both situations involving the hand-carrying meet the requirements stated in this section. Hand-carrying will be authorized only when:

(1) The information is not available at the destination and is required by operational necessity or a contractual requirement.

(2) The information cannot be sent by a secure facsimile transmission, secure email (SIPRNET), or by other approved secure means, for example, USPS Express Mail delivery.

(3) The hand-carry has been authorized by the appropriate official. For hand-carrying within and between the United States, its territories, Canada, or abroad, in rare cases, the authorizing official will be determined by the commander or equivalent, subject to ACOM, ASCC, or DRU approval. For all other areas, approval can be further delegated in writing by commanders of ACOMs, ASCCs, or DRUs. Where delegated, commanders of ACOMs, ASCCs, or DRUs will exercise oversight, during inspections and/or assistance visits by requiring copies of approvals, or by other means, to ensure the requirements of this section are met.

(4) The hand-carry is accomplished aboard a U.S. carrier or a foreign carrier if no U.S. carrier is available, and the information will remain in the custody and physical control of the U.S. escort at all times.

(5) Arrangements have been made for secure storage during overnight stops and similar periods. The material will not be stored in hotels, personal residences, vehicles, or any other unapproved storage location.

(6) A receipt for the material, for all classification levels, is obtained from an appropriate official at the destination and the receipt is returned to the appropriate official at the traveler’s command.

b. Procedures for authorizing contractors working onsite at a command to escort, courier, or hand-carry classified material will comply with the requirements of AR 380–49 (see DoDM 5200.22, Volume 2 and DoD 5220.22–M) and this regulation.

##### **7–12. Documentation**

a. Responsible officials will provide a written statement authorizing such transmission, which will be acknowledged by signature by individuals escorting or carrying classified material. This may be satisfied by either a briefing or written instructions and will include 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 will be made for storage of the classified material at a U.S. military facility, embassy, or cleared contractor facility. Classified information will not be stored in hotel safes.

(3) The material will not be opened en route except in cases of emergency.

(4) The material will not be discussed or disclosed in any public place.

(5) The individual will not deviate from the authorized travel schedule.

(6) In cases of emergency, the individual will take measures to protect the material.

(7) The individual is responsible for ensuring personal travel documents (passport, courier authorization (if required), and medical documents) are complete, valid, and current.

b. The DD Form 2501 (Courier Authorization) may be used to identify appropriately cleared DA personnel who have been approved to hand-carry classified material in accordance with the following, except that in the case of travel aboard commercial aircraft, the provisions of paragraph 7–13 of this regulation apply:

- (1) The individual has a recurrent need to hand-carry classified information;
- (2) The form is signed by an appropriate official in the individual's servicing security office;
- (3) Stocks of the form are controlled to preclude unauthorized use.
- (4) The form is issued no more than 2 years at a time. The requirement for authorization to hand-carry will be reevaluated and/or revalidated on at least a biennial basis, and a new form issued, if appropriate.
- (5) Only the last four digits of the individual's social security number will be used when filling out the DD Form 2501.

(6) The use of the DD Form 2501 for identification and/or verification of authorization to hand-carry SCI or SAP information will be in accordance with policies and procedures, established by the official having security responsibility for such information or programs.

### **7–13. Hand-carrying or escorting classified material aboard commercial passenger aircraft**

a. 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.

b. The individual designated as the courier will possess a DoD or contractor-issued common access card (CAC) 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.)

c. The courier will have courier orders (letter prepared on letterhead stationery of the agency authorizing the carrying of classified material), which will include:

- (1) The full name of the individual and his or her DA command or company.
- (2) A date of issue and an expiration date.
- (3) The name, title, signature, and phone number of the official issuing the letter.
- (4) The name of the person and official government telephone number of the person designated to confirm the courier authorization.

d. Upon arrival at the screening checkpoint, the individual designated as the courier will ask to speak to the TSA Supervisory Transportation Security Officer and will present the required identification and authorization documents. If the courier does not present all required documents, including valid courier authorization, DoD or contractor-issued CAC, and government-issued photo identification card, TSA officials will require the classified material to be screened in accordance with its standard procedures.

e. The courier will 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 government classified material is exempted from any form of inspection; the courier and all of the courier's personal property will be provided for screening. The classified material will 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.

f. Hand-carrying classified items aboard international commercial aircraft will be conducted only on an exception basis. DA personnel requiring access to classified materials at an overseas location will exhaust all other transmission options (for example, electronic file transfer, advance shipment by courier) before hand-carrying items aboard international commercial aircraft. In addition to the requirements in paragraphs 7–13a through 7–13e, for international travel, the authorization letter will describe the material being carried (for example, "three sealed packages (9" x 8" x 24")," addressee, and sender) and the official who signed the authorization letter will sign each package or carton that is exempt to facilitate its identification.

g. There is no assurance of immunity from search by the customs, police, and/or immigration officials of the various countries whose border the traveler may be crossing. Therefore, should such officials inquire into the contents of the consignment, the traveler will present the courier orders and ask to speak to the senior customs, police, and/or immigration official. This action should normally suffice to pass the material through unopened. However, if the senior customs, police, and/or immigration official demands to see the actual contents of the package, it should be opened only in his/her presence, and must be done in an area out of sight of the general public, if possible. If the traveler is permitted to pass, notification to his/her command will be done at the earliest possible time.

(1) Precautions must be taken to show officials only as much of the contents as will satisfy them that the package does not contain any other item. The traveler should ask the official to repack or assist in repackaging of the material immediately upon completion of the examination.

(2) The senior customs, police, and/or immigration official, should be requested to provide evidence of the 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.

(3) If the package has been opened under such circumstances as those mentioned above, the traveler will inform, in writing, the addressee and the dispatching security officer of this fact.

(4) Prior to travel, classified material to be carried by a traveler will be inventoried and a copy of the inventory retained by the traveler's security office. A copy of the inventory will be placed inside the classified package.

*h.* For guidance on hand-carrying NATO information, travelers who are authorized to carry NATO classified material on international flights will refer to USSAN 1-07.

## **7-14. Consignor/consignee responsibility for shipment of bulky material**

The consignor of a bulk shipment will—

*a.* Select a carrier that will provide a single line service from the point of origin to destination when such a service is available.

*b.* Ship packages weighing less than 200 pounds in closed vehicles only.

*c.* Notify the consignees and military transshipping activities of the nature of the shipment, including level of classification, the means of shipment, the serial number of the seals, if used, and the anticipated time and date of arrival by separate communication, at least 24 hours in advance of arrival of the shipment.

*d.* Advise the first military transshipping activity that, if the material does not move on the conveyance originally anticipated, the transshipping activity should advise the consignee with information of the firm date and estimated time of arrival. Upon receipt of the advance notice of a shipment of classified material, consignees and transshipping activities will take appropriate steps to receive the classified shipment and to protect it upon arrival.

*e.* Annotate the bills of lading to require the carrier to notify the consignor immediately, by the fastest means, if the shipment is unduly delayed in route. Such annotations will not under any circumstances disclose the classified nature of the commodity. When seals are used, annotate substantially as follows: "DO NOT BREAK SEALS EXCEPT IN EMERGENCY OR UPON AUTHORITY OF CONSIGNOR OR CONSIGNEE. IF BROKEN, APPLY CARRIER'S SEALS AS SOON AS POSSIBLE AND IMMEDIATELY NOTIFY CONSIGNOR AND CONSIGNEE."

*f.* Require the consignee to advise the consignor of any shipment not received more than 48 hours after the estimated time of arrival furnished by the consignor or the transshipping activity. Upon receipt of such notice, the consignor will immediately trace the shipment. If there is evidence that the classified material was subjected to compromise, the procedures set forth in chapter 9 of this regulation for reporting compromises will apply.

## **Chapter 8 Security Education and Training**

### **Section I**

#### **Policy**

#### **8-1. General policy**

*a.* Commanders will establish security education programs. These programs will be aimed at promoting quality performance of security responsibilities by command personnel and will be tailored, as much as possible, to the specific involvement of individuals in the information security program and the command's mission. The programs will—

(1) Provide necessary knowledge and information to enable quality performance of security functions.

(2) Promote understanding of information security program policies and requirements, and their importance to the national security.

(3) Instill and maintain continuing awareness of security requirements and the intelligence collection threat.

(4) Assist in promoting a high degree of motivation to support program goals.

*b.* The DCS, G-2, has released standardized web-based security training products that can be used and will satisfy the requirements outlined below for initial security orientation and annual refresher training. Training is available on the Army Learning Management System (ALMS) through Army Knowledge Online.

c. Commanders will ensure training programs include annual CUI training requirements outlined in DoDI 5200.48. DoD's CUI training can be accessed at <https://www.dodcui.mil/home/training/> may be combined into the overall program addressing both classified and CUI.

## **8-2. Methodology**

Security education must be a continuous, rather than periodic, influence on individual security performance. Periodic briefings, training sessions, and other formal presentations will be supplemented with other informational and promotional efforts to ensure maintenance of continuous awareness and performance quality. The use of external resources, such as the training products produced by the DCSA, Center for Development of Security Excellence (CDSE), may be used 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 will not be considered as fulfilling any of the specific requirements of this chapter, because there is no basis to gauge effectiveness.

## **Section II**

### **Briefings and Training**

#### **8-3. Initial security orientation**

a. All DA personnel will be given an initial security orientation whether cleared for access to classified information or not. The purpose of the orientation will be:

- (1) To define classified information and CUI and explain the importance of protecting such information.
- (2) To develop a basic understanding of security policies and principles.
- (3) To ensure personnel are aware of the roles they are expected to play in the information security program, and inform them of the administrative, civil, and/or criminal sanctions that can be applied when appropriate.
- (4) To provide personnel with enough information to ensure the proper protection of classified information and CUI that is in their possession, including the actions to be taken if such information is discovered unsecured, a security vulnerability is noted, or when a person may be seeking unauthorized access to the information.

(5) To inform personnel of the requirement for review of all unclassified information prior to release to the public.

b. In addition to paragraph 8-3a, DA personnel, upon initial access to classified information, will receive training on security policies and principles and derivative classification practices. The training is intended to:

- (1) Develop a basic understanding of the nature of classified information and the importance of its protection to the national security.
- (2) Provide personnel enough information to ensure proper protection of classified information in their possession. Security educators will, at a minimum, include the following points in their Security education programs:
  - (a) The nature of U.S. and FGI classified information, its importance to the national security, and the degree of damage associated with each level of classification/sensitivity.
  - (b) How to recognize U.S. and FGI classified information that personnel may encounter, including their marking.
  - (c) The individual's responsibility for protection of classified information and the consequences of failing to do so.
  - (d) Procedures and criteria for authorizing access to classified information.
  - (e) Procedures for safeguarding and control of classified information in the individual's work environment.
  - (f) Proper response to discovery of information believed to be classified in the public media.
  - (g) The security management and support structure within the command, to include sources of help with security problems and questions and proper procedures for challenging classifications believed to be improper.
  - (h) Penalties associated with careless handling or compromise of classified information.

c. Before being granted access to classified information, employees must sign SF 312. See paragraph 5-2 of this regulation for details regarding the use of the SF 312.

#### **8-4. Annual refresher training**

Security education programs will include efforts to maintain and reinforce quality performance of security responsibilities. At a minimum, all DA personnel will receive annual security refresher training that reinforces the policies, principles, and procedures covered in their initial and specialized training. In addition to the web-based training available and discussed in para 8-1b, security educators should also supplement this training by addressing issues or concerns identified during self-inspections. Whenever security policies and procedures change, personnel, whose duties would be impacted by these changes, must be briefed as soon as possible.

### **8–5. Training for managers and supervisors**

Web-based information security training will be completed initially and yearly thereafter for civilian supervisors, officers, and enlisted personnel in the grade of corporal and above who manage personnel with security clearances and access to classified information (see para 8–1*b* and AR 350–1). This training is available on ALMS and is currently titled, “Annual Awareness–Managing Soldiers and Civilians with Security Clearance/Access.”

## **Section III**

### **Special Requirements**

### **8–6. General policy**

DA personnel in positions which require performance of specified roles in the information security program will be provided security training sufficient to permit quality performance of those duties. The training will be provided before, concurrent with, or not later than 6 months following assumption of those positions, unless otherwise specified in this regulation.

### **8–7. Original classifiers**

*a.* Training for newly appointed OCAs will be provided before they exercise the delegated authority and annually thereafter. The OCA will certify in writing that the training was received. Personnel preparing recommendations for original classification to OCAs will receive the same training. The training will 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. Additional policies and procedures on what training must address can be found in DoDM 5200.01, Volume 3.

*b.* Security educators may consider the use of job aids or similar techniques, for example, video tapes or self-paced computer training programs, to replace or supplement traditional educational techniques due to the relatively low frequency of training for original classification authorities. The DCSA, CDSE provides up-to-date training resources for OCA training that may be used to meet training requirements outlined above. Training can be found at <https://www.cdse.edu/index.html>.

*c.* DoDM 5200.45 can be used as a reference for OCAs in making original classification decisions and is required for developing command-level SCGs.

### **8–8. Derivative classifiers**

*a.* DA personnel, whose responsibilities include derivative classification, will be trained yearly in requirements and procedures appropriate to the information and material they will be classifying, including the proper use of classification guides and source documents (see para 2–6). Training will address the following topics:

- (1) What are the original and derivative classification processes and the standards applicable to each?
  - (2) What are the proper and complete classification markings to be applied to classified information?
  - (3) What are the authorities, methods, and processes for downgrading and declassifying information?
  - (4) What are the methods for the proper use, storage, reproduction, transmission, dissemination, and destruction of classified information?
  - (5) What are the requirements for creating and updating classification and declassification guides?
  - (6) What are the requirements for controlling access to classified information?
  - (7) What are the procedures for investigating and reporting instances of actual or suspected compromise of classified information and the penalties that may be associated with violation of established security policies and procedures?
  - (8) What are the procedures for the secure use, certification, and accreditation of ISs and networks which use, process, store, reproduce, or transmit classified information?
  - (9) What are the requirements for oversight of the security classification program, including self-inspections?
- b.* Derivative classification training is in addition to the training outlined in paragraph 8–1*b*.

### **8–9. Security program management personnel**

Individuals designated as SMs, classification management officers, security specialists, or any other personnel whose duties involve managing or overseeing classified information will receive training that meets the requirements of DoDI 3305.13. The training and education should be tailored to suit their expected contributions to the program and will include at a minimum:



- a.* Procedures, standards, and processes for original and derivative classification, and for downgrading and declassifying information.
- b.* Proper and complete classification markings to be applied to classified information.
- c.* Proper use of control markings to limit or expand distribution, including foreign disclosure and release markings.
- d.* Requirements and techniques for controlling access to classified information and for the proper use, storage, reproduction, transmission, transportation, dissemination, and destruction of classified material.
- e.* The authorities, methods, and processes for downgrading and declassifying information.
- f.* Procedures and requirements for investigating and reporting instances of actual or suspected compromise of classified information, including in electronic form, and the penalties that may be associated with violating established security policies and procedures.
- g.* Requirements and procedures for securing classified information processed, maintained, or stored on ISs.
- h.* The SM and select security staff personnel will be educated in at least the basics of IS security to support a seamless, integrated security program.
- i.* Requirements and methods for security education, program oversight, and program management.

#### **8–10. North Atlantic Treaty Organization briefing for cleared personnel**

To facilitate potential access to NATO classified information, DA personnel who are briefed on their responsibilities for protecting U.S. classified information will be briefed simultaneously on the requirements for protecting NATO information. A written acknowledgment of the individual's receipt of the NATO briefing and responsibilities for safeguarding NATO classified information will be maintained on file. As stipulated in USSAN 1–07, access to NATO classified information will require a supervisor's determination of the individual's need-to-know and possession of the requisite security clearance. Receipt of the NATO briefing will be verified prior to granting access to NATO classified information.

#### **8–11. Others**

Commanders of ACOMs, ASCCs, and DRUs will include in their security education programs, either in the general program or as part of special briefings to select personnel affected, provisions regarding special education and training for personnel who:

- a.* Use ISs to store, process, or transmit classified information (see AR 25–2).
- b.* Will be traveling to foreign countries where special concerns about possible exploitation exist or will be attending professional meetings or conferences where foreign attendance is likely. The military intelligence unit providing counterintelligence (CI) support to the command should be contacted for assistance and/or information in this regard.
- c.* Will be escorting, hand-carrying, or serving as a courier for classified information and material.
- d.* Are authorized access to classified and/or sensitive information requiring special control or safeguarding measures.
- e.* Are involved with international programs.
- f.* Regardless of security clearance eligibility and/or access level held, all DA personnel will receive Threat Awareness and Reporting Program training yearly, as required and in accordance with AR 381–12.

#### **8–12. Termination briefings**

DA commands will establish procedures to make sure that cleared employees, who leave the command or whose security clearance eligibility is terminated, receive a termination briefing. See paragraph 5–5 of this regulation for more detailed policy on termination briefings. This briefing will—

- a.* Emphasize a continued responsibility to protect classified and CUI 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 CUI material when leaving the organization.
- d.* Identify the requirement that retired personnel, former DA personnel, and members of the Reserve Components not serving on active duty must submit writings and other materials intended for public release to the DoD prepublication review process as specified in DoDI 5230.09.
- e.* Remind them of the potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

### **8–13. Program management**

Commanders will ensure that their security education and training programs are appropriately evaluated during self-inspections and during oversight activities of subordinate commands or organizational units. This evaluation will include assessment of the quality and effectiveness of security education efforts, as well as ensuring appropriate coverage of the target populations. Commands will maintain a record of the programs offered and of the personnel that participated. These records will be maintained for 2 years and will be available for review during oversight inspections and assistance visits.

## **Chapter 9**

### **Security Incidents and Reporting Involving Classified Information**

#### **Section I**

#### **Policy**

#### **9–1. Terms and categories of security incidents**

- a. The terms associated with a security incident are formally defined in DoDM 5200.01, Volume 3.
- b. Certain types of classified information or specific circumstances require unique handling or consideration of additional reporting requirements as specified below. Actual or possible compromises involving:
  - (1) COMSEC or cryptographic information will be handled in accordance with AR 380–40.
  - (2) SCI will be handled in accordance with DoDM 5105.21 (see AR 380–28).
  - (3) SAP information will be handled through SAP channels in accordance with AR 380–381.
  - (4) FGI and NATO information will be reported to the Office of the Under Secretary of Defense (Policy), (OUSD (P)). These reports will be made through command channels through the DCS, G–2 (DAMI–CD).
  - (5) Classified information involving IT, ISs, computer systems, terminals, or equipment will be reported in accordance with AR 25–2 through appropriate channels by the information assurance manager to the SM. Inquiries into and the resolution of incidents involving compromise of classified information residing on computers or IT systems require coordination between information assurance personnel and security personnel.
  - (6) Any incidents in which a deliberate compromise of classified information or involvement of a foreign intelligence service, international terrorist group, or organization is suspected will be reported to the appropriate Army CI agency in accordance with AR 381–12. Commands will not initiate or continue an inquiry or investigation of a security incident unless it is fully coordinated with the Army CI agency.
  - (7) Security incidents involving RD and/or FRD. In accordance with 50 USC 2672(e), the Secretary of Energy must report to the Senate Armed Services Committee, House Armed Services Committee, and Assistant to the President for National Security Affairs any inadvertent releases of RD or FRD occurring pursuant to automatic declassification processes. Commanders of ACOMs, ASCCs, and DRUs will notify the Secretary of the DOE as necessary and provide a copy of the notification to the DCS, G–2 (DAMI–CD) for reporting to the Deputy Assistant Secretary of Defense for Nuclear Matters and the Director of Security, OUSD (I).
  - (8) 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 9–1b(3), will be reported immediately to the U.S. Army Criminal Investigation Command (CID). If CID accepts jurisdiction and initiates an investigation, the reporting organization will not initiate or continue an inquiry or investigation, so as not to jeopardize the integrity of the CID investigation.
  - (9) Security incidents involving classified United States information provided to foreign governments. Actual or suspected compromise of U.S. classified information held by foreign governments will be reported to the originating command, the OCA, through the DCS, G–2 (DAMI–CD) to the Director of Security, OUSD (I), and the Director, International Security Programs, Defense Technology Security Administration, OUSD (P).
  - (10) Security incidents involving improper transfer of classified information. Any DA command or organization that receives classified information that has been improperly handled, addressed, packaged, transmitted, or transported will make a determination as to whether the information has been subjected to compromise. If the command determines that the classified information has been subjected to compromise, the receiving command will immediately notify the sending activity, which will be responsible for initiating an inquiry or investigation, as appropriate. The receiving command will share information generated regarding the incident with the sending activity. The sending activity is responsible for required notifications (for example, to the OCA). Classified information will 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 (for example, telephone,

facsimile, message, email, computer, or data links) over communications circuits that are not approved for transmission of classified information. If the receiving activity determines classified information was not in fact compromised, but was nevertheless improperly prepared or transferred, the receiving activity will report the discrepancy to the sending activity.

(11) Security incidents involving contractors. Security incidents, including any inquiries or investigations required involving contractors that are embedded/integrated will be handled in accordance with AR 380–49. Disciplinary action and sanctions are the responsibility of the contractor’s company unless specific contract provisions address such actions. SMs will furnish the results of inquiries to the company, with a copy to DCSA, to facilitate such action.

(12) Security incidents involving CPI. Upon learning that classified CPI or CPI related to classified contracts may have been or was actually compromised, security officials will inform the program manager of record and the cognizant Army CI agency.

## **9–2. Reporting and notifications**

*a.* Anyone finding classified material out of proper control will take custody of and safeguard the material, if possible, and immediately notify the appropriate security authorities. In all cases, the individual’s immediate supervisor must be notified.

*b.* Any person who becomes aware of the possible loss or potential compromise of classified information will immediately report it to the commander, SM, or other official the commander may direct.

*c.* If the person believes the commander, SM, or other official designated to receive such reports may have been involved in the incident, the person making the discovery will report it to the security authorities at the next higher level of command or supervision.

*d.* Security incidents involving the following will be reported immediately through command channels to DCS, G–2 (DAMI–CD). Where appropriate, a preliminary report will be provided outlining the facts, particularly when the incident may become public or attract media attention. DCS, G–2 (DAMI–CD), will be notified of:

(1) A violation involving espionage.

(2) An unauthorized disclosure of classified information in the public media. See DoDM 5200.01, Volume 3 for further procedures and information required in the notification. Additional notification is not required for reference to or republication of a previously identified media disclosure.

(3) Any violation wherein properly classified information is knowingly, willfully, or negligently disclosed to unauthorized persons or when information is marked or is continued as classified in violation of this regulation:

(*a*) Is reported to the oversight committees of Congress;

(*b*) May attract significant public attention;

(*c*) Involves large amounts of classified information; or

(*d*) Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(4) Any violation wherein an SAP is knowingly, willfully, or negligently created or continued contrary to the requirements of AR 380–381, DoD policies, and national policies.

(5) 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 10 USC 2723.

*e.* Security incidents that do not meet the reporting criteria specified above will be filed in a retrievable format by the command and will be available for inspection or for further analysis, review, and potential investigation.

## **9–3. Security inquiries and investigations**

When an incident of actual or suspected compromise of classified information is reported, the commander will immediately initiate a written inquiry to determine the facts and circumstances of the incident, and to characterize the incident as an infraction or a violation.

*a.* Report of inquiry will be completed in accordance with DoDM 5200.01, Volume 3. The person appointed to conduct the inquiry will have the appropriate security clearance and accesses, the ability and available resources to conduct an effective inquiry, and will not be likely to have been involved, directly or indirectly, in the incident. Except in unusual circumstances, the SM will not be appointed to conduct the inquiry. It is typically the responsibility of the SM, unless command policy states otherwise, to ensure that an official is appointed to conduct the inquiry and that the inquiry is completed. Advice and assistance may be requested from the supporting CI organization.

*b.* Inquiry reports will be classified, appropriately marked, and handled according to their content; at a minimum, controlled as CUI.

c. The inquiry will be initiated and completed as soon as possible but not to exceed 10 duty days, and the report of findings will be provided to the commander, SM, and others, as appropriate, and in accordance with this regulation and local command policy and procedures.

d. The person appointed to conduct the inquiry will notify the OCA, or the originator when the OCA is not known, when it is determined there is a compromise, suspected compromise, or loss of classified information. The OCA will then take actions as required in DoDM 5200.01, Volume 3.

e. If, at any time during the inquiry, it appears that deliberate compromise of classified information may have occurred, the inquiry will stop and the incident will be immediately reported to the chain of command and supporting CI unit. Apparent violations of other criminal law will be reported to the supporting CID. In both cases, coordination with the command's legal counsel is required.

f. If the report from the inquiry is not sufficient to resolve the security incident, the command will initiate an investigation under the provisions of AR 15–6. The inquiry report will become part of any formal investigation. Report of investigation will be completed in accordance with DoDM 5200.01, Volume 3. If the inquiry is closed out as a compromise or suspected compromise, the appointing authority will notify the OCA to perform a damage assessment.

#### **9–4. Classified information appearing in the public media**

a. If classified information appears in the public media, including public internet sites, or if approached by a representative of the media, DA personnel will not make any statement or comment that confirms the accuracy of or verify the classified status of the information. Personnel will report the approach immediately to the appropriate command, security, and public affairs personnel.

(1) It is essential that DA personnel are careful to neither confirm nor deny the existence of classified information or the accuracy of such information in the public media.

(2) The news article or other medium will not be marked as classified; however, the written report detailing the discovery of the information in the public media will be classified to the level of the information believed to have been compromised. Personnel will not discuss the matter with anyone without the express approval of the SM or an individual so designated by the SM or commander. An appropriate security clearance and need-to-know is required. No discussions will be made over nonsecure circuits.

b. Notifications of unauthorized disclosures of classified information in the public media required by paragraph 9–2d will be completed in accordance with DoDM 5200.01, Volume 3.

#### **9–5. Reporting results of the inquiry**

a. If the inquiry concludes that a compromise could have occurred or that a compromise did occur and damage to the national security can result, the official initiating the inquiry will immediately notify the originator of the information or material involved. If the originator was not the OCA, the OCA will also be immediately notified. If the originator cannot be determined, the commander of the ACOM, ASCC, or DRU will be contacted for guidance. The commander of the ACOM, ASCC, or DRU will contact the DCS, G–2 (DAMI–CD), for those cases in which the ACOM, ASCC, or DRU cannot direct the command to the appropriate activity. Notification of the originator and OCA will not be delayed pending completion of any additional inquiry or resolution of other related issues.

b. If the conclusion of the inquiry is as stated in para 9–5a, the command will report the matter through command channels to its ACOM, ASCC, or DRU, or to the AASA. The commander of the ACOM, ASCC, or DRU or the AASA will review the report for completeness and adequacy of the investigation. Such reports will be filed and retained for a period no less than 2 years and are subject to HQDA or other appropriate agency oversight.

#### **9–6. Reevaluation and damage assessment**

When notified of possible or actual compromise, the holder of the information or material will ensure that the command with the OCA for each item of the information is notified of the incident. The OCA will verify and reevaluate the classification of the information and will conduct a damage assessment in accordance with DoDM 5200.01, Volume 3.

#### **9–7. Debriefings in cases of unauthorized access**

When a person has had unauthorized access to classified information, it is advisable to discuss the situation with the individual to enhance the probability that he or she will appropriately protect it. Whether such a discussion, commonly called a “debriefing,” is held, is to be decided by the commander, SM, or other designated official. This decision must be based on the circumstances of the incident, what is known about the person(s) involved, and the nature of the classified 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 unnecessary. Debriefing is required if the individual is not aware the information is classified and that it needs protection. Inform the person the information is classified and it requires protection. In these cases, the signing of a debriefing statement is usually not necessary (see para 9–7e).

*b.* If the unauthorized access was by U.S. Government civilian or military personnel without the appropriate security clearance, debriefing will be accomplished. Personnel will be advised of their responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties which might follow if they fail to do so. The debriefing official will make sure the individual understands what classified information is and why its protection is important.

*c.* If the person who had unauthorized access is an employee of a cleared U.S. Government contractor participating in the National Industrial Security Program, the same guidelines apply as for U.S. Government personnel. Coordination with the employing firm's facility security officer is recommended unless such coordination would place the information at increased risk.

*d.* If the person involved is neither U.S. Government personnel, nor an employee of a cleared U.S. Government contractor, the decision will be made by the commander. The key question to be decided is whether the debriefing will have any likely positive effect on the person's ability and/or willingness to protect the information. As a general rule, it is often more effective in the long run to explain a mistake occurred and the person had unauthorized access to certain sensitive government information, which should not have happened and the U.S. Army needs the individual to understand the information must be protected and never further discussed or otherwise revealed to other unauthorized personnel.

*e.* It is useful to have the person being debriefed sign a statement acknowledging the debriefing and its contents. If, when asked, the person refuses to sign a debriefing statement, this fact, and his or her stated reasons for refusing, will be made a matter of record in the inquiry. The nearest CI unit will immediately be notified so that a trained CI investigator can explain the reason for the debriefing and advise the individual that a refusal to sign could indicate an unwillingness to protect classified information and could place his or her clearance, if held at the time, in jeopardy.

*f.* If the person being debriefed may be the subject of criminal prosecution or disciplinary action, command officials are advised to consult with legal counsel before attempting to debrief the individual.

## **9–8. Management and oversight**

*a.* Commanders of ACOMs, ASCCs, DRUs, and the AASA will establish internal reporting and oversight mechanisms, to ensure inquiries and/or investigations are conducted when required, that they are done in a timely and effective manner, and that appropriate management action is taken to correct identified problem areas.

*b.* Inquiries and management analyses of security incidents will consider possible systemic shortcomings which could have caused or contributed to the incident. The effectiveness of command security procedures, security education, supervisory oversight of security practices, and command management emphasis on security will be considered when determining causes and contributing factors. The focus of management's response to security incidents will be to eliminate or minimize the possibility of further incidents occurring.

*c.* Disciplinary action or criminal prosecution, discussed in chapter 1, section VI, of this regulation, is one means of addressing incidents, but the broader focus on prevention must not be lost. Disciplinary action will not be the sole reaction to a security incident, unless there has been a consideration of what other factors may have contributed to the situation.

*d.* Commands will establish a system of controls and procedures to make sure reports of security inquiries and damage assessments are conducted, when required, and the results are available as needed. Such reports will be available for review during inspections and oversight reviews. Commanders of ACOMs, ASCCs, DRUs, and the AASA can establish reporting requirements for such inquiries and assessments.

## **9–9. Unauthorized absences, suicides, or incapacitation**

When an individual who has or had access to classified information is absent without authorization, commits or attempts to commit suicide, or is temporarily or permanently incapacitated, the command will inquire into the situation to see if there are indications of activities, behavior, or associations that could indicate classified information might be at risk. If so, the supporting CI organization will be notified. The scope and depth of this inquiry will depend on the length of the absence, factors leading to the actual or attempted suicide or reasons and causes for the incapacitation, and the sensitivity of the classified information involved. See AR 190–45 for further details.

**9–10. Negligence**

DA personnel are subject to administrative or disciplinary sanctions if they negligently disclose to unauthorized persons information properly classified under EO 13526 or any prior or subsequent order. Administrative or disciplinary action against U.S. military personnel can be pursued but is not required. Administrative or disciplinary action against DA Civilian personnel can be pursued under DA Civilian personnel regulations but is not required. No action is to be taken without advice of servicing legal counsel and until a full inquiry has been completed to determine the seriousness of the incident.

## Appendix A

### References

#### Section I

##### Required Publications

Army publications are available on the Army Publishing Directorate website at <https://armypubs.army.mil/>. DoD issuances are available on the Executive Services Directorate website at <https://www.esd.whs.mil/dd/>.

##### **AR 25–400–2**

The Army Records Information Management System (ARIMS) (Cited in para 3–5a.)

##### **DoDI 5200.48**

Controlled Unclassified Information (CUI) (Cited on title page.)

##### **DoDM 5200.01, Volume 1**

DoD Information Security Program: Overview, Classification, and Declassification (Cited in para 1–15a(2).)

##### **DoDM 5200.01, Volume 2**

DoD Information Security Program: Marking of Information (Cited in para 1–15a.)

##### **DoDM 5200.01, Volume 3**

DoD Information Security Program: Protection of Classified Information (Cited in para 1–8d.)

##### **DoDM 5200.45**

Instructions for Developing Security Classification Guides (Cited in para 2–17.)

##### **EO 13526**

Classified National Security Information (Available at <https://www.archives.gov/>.) (Cited in the title page.)

##### **EO 13556**

Controlled Unclassified Information (Available at <https://obamawhitehouse.archives.gov/>.) (Cited in para 1–1.)

#### Section II

##### Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website (<https://armypubs.army.mil/>), DoD issuances are available on the Executive Services Directorate website (<https://www.esd.whs.mil/dd/>). EOs are available at <https://www.archives.gov/>. The USC is available at <https://us-code.house.gov/>.

##### **AR 11–2**

Managers' Internal Control Program

##### **AR 15–6**

Procedures for Administrative Investigations and Boards of Officers

##### **AR 25–2**

Army Cybersecurity

##### **AR 25–30**

Army Publishing Program

##### **AR 25–55**

The Department of the Army Freedom of Information Act Program

##### **AR 27–10**

Military Justice

##### **AR 27–40**

Litigation

##### **AR 190–13**

The Army Physical Security Program

**AR 190–45**

Law Enforcement Reporting

**AR 195–2**

Criminal Investigation Activities

**AR 350–1**

Army Training and Leader Development

**AR 360–1**

The Army Public Affairs Program

**AR 380–10**

Foreign Disclosure and Contacts with Foreign Representatives

**AR 380–27**

Control of Compromising Emanations

**AR 380–28**

Army Sensitive Compartmented Information Security Program

**AR 380–40**

Safeguarding and Controlling Communications Security Material (U)

**AR 380–49**

Industrial Security Program

**AR 380–53**

Communications Security Monitoring

**AR 380–67**

Personnel Security Program

**AR 380–381**

Special Access Programs (SAPs) and Sensitive Activities

**AR 381–12**

Threat Awareness and Reporting Program

**AR 525–13**

Antiterrorism

**AR 530–1**

Operations Security

**AR 600–8–104**

Army Military Human Resource Records Management

**CNSSI No. 4004.1**

Destruction and Emergency Protection Procedures for COMSEC and Classified Material (Available at <https://www.cnss.gov/cnss/>.)

**DA Pam 25–403**

Guide to Recordkeeping in the Army

**DoD 5220.22–M**

National Industrial Security Program Operating Manual

**DoDD 3020.40**

Mission Assurance (MA)

**DoDD 5000.01**

The Defense Acquisition System

**DoDD 5142.01**

Assistant Secretary of Defense (Legislative Affairs) (ASD(LA))



**DoDD 5210.50**

Management of Serious Security Incidents Involving Classified Information

**DoDD 5230.11**

Disclosure of Classified Military Information to Foreign Governments and International Organizations

**DoDD 5230.20**

Visits and Assignments of Foreign Nationals

**DoDD 5405.2**

Release of Official Information in Litigation and Testimony by DoD Personnel As Witnesses

**DoDI 3305.13**

DoD Security Education, Training, and Certification

**DoDI 5000.02T**

Operation of the Defense Acquisition System

**DoDI 5200.33**

Defense Courier Operations (DCO)

**DoDI 5200.39**

Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)

**DoDI 5210.02**

Access to and Dissemination of Restricted Data and Formerly Restricted Data

**DoDI 5210.83**

DoD Unclassified Controlled Nuclear Information (UCNI)

**DoDI 5230.09**

Clearance of DoD Information for Public Release

**DoDI 5230.24**

Distribution Statements on Technical Documents

**DoDI 5230.29**

Security and Policy Review of DoD Information for Public Release

**DoDI 5240.04**

Counterintelligence (CI) Investigations

**DoDI 5400.04**

Provision of Information to Congress

**DoDI 5400.11**

DoD Privacy and Civil Liberties Program

**DoDI 5505.02**

Criminal Investigations of Fraud Offenses

**DoDI 7650.01**

Government Accountability Office (GAO) and Comptroller General Requests for Access to Records

**DoDM 5105.21 Volumes 1 through 3**

Sensitive Compartmented Information (SCI) Administrative Security Manual

**DoDM 5200.02**

Procedures for the DoD Personnel Security Program (PSP)

**DoDM 5220.22, Volume 2**

National Industrial Security Program: Industrial Security Procedures for Government Activities

**EO 12333**

United States intelligence activities

**EO 13549**

Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities

**FED-STD-809D**

Inspection, Maintenance, Neutralization and Repair of GSA Approved Containers and Vault Doors (Available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).)

**Federal Specification AA-F-358J**

Filing Cabinet, Legal and Letter Size, Uninsulated, Security (Available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).)

**Federal Specification AA-V-2737**

Modular Vault Systems (Available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).)

**Federal Specification FED-STD 832**

Construction Methods and Materials for Vaults (Available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).)

**Federal Specification FF-L-2740B**

Locks, Combination, Electromechanical (Available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).)

**Federal Specification FF-L-2937**

Mechanical Combination Locks (Available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).)

**Federal Specification FF-P-110**

Combination Padlocks (Available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).)

**MIL-HDBK-1013/1A**

Design Guidelines for Physical Security of Facilities (Available at [https://www.navfac.navy.mil/navfac\\_worldwide/specialty\\_centers/exwc/products\\_and\\_services/capital\\_improvements/dod\\_lock.html](https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html).)

**NSA/CSS EPL 02-01**

NSA/CSS Evaluated Products List for High Security Crosscut Paper Shredders (Available at <https://www.nsa.gov/>.)

**NSA/CSS EPL 02-02**

NSA/CSS Evaluated Products List for High Security Disintegrators (Available at <https://www.nsa.gov/>.)

**NSA/CSS Policy Manual No. 3-16**

Control of Communications Security (COMSEC) Material (Available to authorized recipients at [www.iad.nsa.smil.mil/resources/library/nsa\\_office\\_of\\_policy\\_section/index.cfm](http://www.iad.nsa.smil.mil/resources/library/nsa_office_of_policy_section/index.cfm).)

**NSTISSI 7003**

Protected Distribution Systems (Available at <https://www.cnss.gov/>.)

**UL Standard 634**

Standard for Connectors and Switches for Use with Burglar-Alarm Systems (Available at <https://standardscatalog.ul.com/>.)

**U.S. Office of Personnel Management Operating Manual**

The Guide to Personnel Recordkeeping (Available at <https://www.opm.gov/>.)

**USSAN Instruction 1-07**

Implementation of NATO Security Requirements (Available from the Central U.S. Registry.)

**Volume 75, Federal Register, p. 735-736**

Original Classification Authority (Available at <https://www.archives.gov>)

**22 CFR Parts 120 through 130**

International Traffic in Arms Regulations (Available at <https://www.ecfr.gov/>.)

**32 CFR 2001.25**

Declassification markings (Available at <https://ecfr.gov>.)

**5 USC**

Government Organization and Employees

**5 USC 522a**

Records maintained on individuals

**10 USC 2723**

Notice to congressional committees of certain security and counterintelligence failures within defense programs

**18 USC**

Crimes and Criminal Procedure

**18 USC 1386**

Keys and keyways used in security applications by the Department of Defense

**35 USC**

Patents

**42 USC 2011 et seq.**

Atomic Energy Act of 1954

**44 USC**

Public printing and documents

**50 USC 2672**

Protection against inadvertent release of Restricted Data and Formerly Restricted Data

**Section III****Prescribed Forms**

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website at <https://armypubs.army.mil/>.

**DA Form 3964**

Classified Document Accountability Record (Prescribed in para 5–18*b*.)

**Section IV****Referenced Forms**

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (<https://armypubs.army.mil/>), DD forms are available on the Executive Services Directorate website (<https://www.esd.whs.mil/directives/forms/>), and **standard** forms are available on the GSA website (<https://www.gsa.gov/>).

**DA Form 11–2**

Internal Control Evaluation Certification

**DA Form 2028**

Recommended Changes to Publications and Blank Forms

**DD Form 2024**

DoD Security Classification Guide Data Elements

**DD Form 2501**

Courier Authorization (must be ordered)

**SF 135**

Records Transmittal and Receipt

**SF 311**

Agency Security Classification Management Program Data

**SF 312**

Classified Information Nondisclosure Agreement

**SF 700**

Security Container Information (must be ordered)

**SF 701**

Activity Security Checklist

**SF 702**

Security Container Check Sheet

**SF 703**

Top Secret Cover Sheet (orange)

**SF 704**

Secret Cover Sheet (red)

**SF 705**

Confidential Cover Sheet (blue)

**SF 715**

U.S. Government Declassification Review Tab (Available at <https://www.archives.gov/isoo/security-forms>)

## Appendix B

### Internal Control Evaluation

#### B-1. Function

This internal control evaluation assesses the command's Information Security Program, including key controls in the following areas: classification, downgrading/upgrading, declassification, marking, transmission, transportation, and safeguarding of classified information.

#### B-2. Purpose

The purpose of this evaluation is to assist commanders and SMs in evaluating key internal controls outlined below. It is not intended to cover all controls nor are all questions listed applicable to all levels of commands.

#### B-3. Instructions

Answers must be based on the actual testing of key internal controls (for example, through document analysis, direct observation, sampling, or other method). Answers that indicate deficiencies must be explained and the corrective action identified in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that the evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification).

#### B-4. Test questions

- a. General provisions and program management.* Does the DCS, G-2 (DAMI-CD):
  - (1) Ensure that policy, procedures, and programs are developed for the implementation of EO 13526 and DoD issuances?
  - (2) Monitor, evaluate, and report on the administration of the Army Information Security Program?
  - (3) Ensure that ACOMs, ASCCs, and DRUs establish and maintain ongoing self-inspection programs that include their subordinate commands, and cover periodic reviews and assessments of their classified and CUI?
  - (4) Coordinate information security matters pertaining to classified material that originated in an ACOM that no longer exists and for which there is no successor in function, where applicable?
  - (5) Delegate Secret and Confidential OCA to other Army officials, where applicable?
  - (6) Commit needed resources for effective policy development and oversight of the programs established by this regulation?
- b. Responsibilities of the commander.* Does the commander—
  - (1) Establish written local information security policies and procedures?
  - (2) Initiate and supervise measures or instructions necessary to ensure continual control of classified information and materials?
  - (3) Ensure that persons requiring access to classified information are properly cleared?
  - (4) Continually assess the individual trustworthiness of personnel who possess a security clearance?
  - (5) Designate an SM by written appointment and of sufficient rank or grade to effectively discharge assigned duties and responsibilities?
  - (6) Ensure the SM is afforded security training consistent with the duties assigned?
  - (7) Ensure adequate funding and personnel are available to allow security management personnel to manage and administer applicable information security program requirements?
  - (8) Review and inspect annually the effectiveness of the Information Security Program in subordinate commands?
  - (9) Ensure prompt and appropriate responses are given or forwarded for higher echelon decision, and any problems, suggestions, requests, appeals, challenges, or complaints arising out of the implementation of this regulation?
- c. Responsibilities of the security manager.* Does the SM—
  - (1) Advise and represent the commander on matters related to the classification, downgrading, declassification, and safeguarding of national security information?
  - (2) Establish and implement an effective security education program as required by chapter 8 of this regulation?
  - (3) Establish procedures for ensuring that all persons handling classified material are properly cleared?
  - (4) Advise and assist officials on classification problems and the development of classification guidance?
  - (5) Ensure that SCGs are properly prepared and maintained?
  - (6) Conduct a periodic review of classifications assigned within the activity to ensure that classification decisions are proper?

- (7) Review all classified documents, in coordination with the organization or command records management officer, to ensure consistency with operational and statutory requirements?
  - (8) Continually reduce, by declassification, destruction, or retirement, unneeded classified material?
  - (9) Submit SF 311 to DCS, G-2 (DAMI-CDS), annually, as required by this regulation?
  - (10) Supervise or conduct security inspections and spot checks and notify the commander regarding compliance with this regulation and other applicable security directives? Assist and advise the commander on matters pertaining to the enforcement of regulations governing the dissemination, reproduction, transmission, safeguarding, and destruction of classified material?
  - (11) Make recommendations on requests for visits by foreign nationals and foreign government representatives? Provide security and disclosure guidance if visit is approved?
  - (12) Ensure the completion of inquiries and the reporting of security violations, including compromises or other threats to the safeguarding of classified information?
  - (13) Advise the decision official concerning potential violations, and/or corrective actions that could be taken concerning security violations?
  - (14) Make sure proposed public releases on classified programs pursuant to the FOIA are reviewed to preclude the release of classified information or CUI?
  - (15) Establish and maintain visit control procedures for visitors who are authorized access to classified information?
  - (16) Issue contingency plans for the emergency destruction of classified information and, where necessary, for the safeguarding of classified information used in or near hostile or potentially hostile areas?
  - (17) Report data as required by this regulation?
- d. Responsibilities of the supervisor.* Does the Supervisor—
- (1) Ensure subordinate personnel who require access to classified information are properly cleared and are given access only to that information for which they have a need-to-know?
  - (2) Ensure subordinate personnel are trained in, understand, and follow the requirements of this regulation and local command policy and procedures concerning the information security program?
  - (3) Continually assess security clearance eligibility for access to classified information of subordinate personnel and report to the SM any information that may have a bearing on that eligibility?
  - (4) Supervise personnel in the execution of procedures necessary to allow the continuous safeguarding and control of classified information?
  - (5) Include the management of classified information as a critical element/item/objective in personnel performance evaluations?
  - (6) Is classified material identified clearly by marking, designations, electronic labeling, or, if physical marking of the medium is not possible, by some other means?
  - (7) Does the SM ensure that marking is completed in accordance with DoDM 5200.01, Volume 2, as stated throughout this regulation?
- e. Classification management.*
- (1) Are personnel designated in writing by either the SECARMY or DCS, G-2, as original classification authorities, where applicable?
  - (2) Are requests for OCA submitted through command channels to DCS, G-2 (DAMI-CD)?
  - (3) Do officials who have been delegated authority as an OCA receive training, as required by chapters 2 and 8 of this regulation, before exercising this authority?
  - (4) Do derivative classifiers make sure that the classification is properly applied based on the original source material marking and local SCGs?
  - (5) Do personnel applying derivative classification:
    - (a) Observe and respect the classification determinations made by original classification authorities?
    - (b) Apply markings or other means of identification to the derivatively classified material, as required by DoDM 5200.01, Volume 2, at the level and for the duration specified by the classification guide or source document?
    - (c) Use only authorized sources, such as classification guides, other forms of official classification guidance, and markings on source material from which the information is extracted, to determine the material's classification?
    - (d) Use caution when paraphrasing or restating information extracted from a classified source to determine whether the classification could have been changed in the process?
    - (e) Make a list of sources used when material is derivatively classified based on "Multiple Sources" (more than one SCG, classified source document, or any combination)? Is a copy of this list included in or attached to the file and/or record copy of the material?

- (f) Contact the classifier of the source document for resolution in cases in which the derivative classifier believes the classification applied to the information is not accurate?
- (6) Are derivative classifiers receiving the required training, as required in chapter 8 of this regulation?
- (7) In making a decision to originally classify an item of information, do OCAs:
- (a) Determine that the information has not already been classified?
  - (b) Determine that the information is eligible for classification pursuant to paragraph 2–8 of this regulation?
  - (c) Determine that classification of the information is a realistic course of action and that it can only be protected from unauthorized disclosure when classified?
  - (d) Decide that unauthorized disclosure of the information could reasonably be expected to cause damage to the National Security that this disclosure is identifiable and can be described?
  - (e) Select the appropriate level or category of classification to be applied to the information, based on a judgment as to the degree of damage unauthorized disclosure could cause?
  - (f) Determine and include the appropriate declassification, and when applicable, downgrading instruction to be applied to the information?
  - (g) Ensure that the classification decision is properly communicated so that the information will receive appropriate protection?
- (8) U.S. classification can only be applied to information that is owned by, produced by or for, or is under the control of the U.S. Government. Does the OCA determine that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and that the information falls within one or more of the categories specified in EO 13526, Section 1.4?
- (9) Does the OCA determine that, if classification is applied or reapplied, there is a reasonable possibility that the information will be provided protection from unauthorized disclosure?
- (10) Once a decision is made to classify, information will be classified at one of three levels. For each level, is the OCA able to identify or describe the damage that unauthorized disclosure reasonably could be expected to cause to the national security?
- (11) Is information declassified as soon as it no longer meets the standards for classification?
- (12) At the time of original classification, does the OCA attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information?
- (13) Is a SCG issued for each, plan, program, project, or operation in which classified information is involved?
- (14) Do SCGs, at a minimum, include the information outlined in paragraph 2–18?
- (15) Are SCGs personally approved in writing by the OCA who is authorized to classify information at the highest level designated by the guide, and who has program support or supervisory responsibility for the information or for the organization's Information Security Program?
- (16) Are SCGs distributed to those commands, contractors, or other activities expected to be derivatively classifying information covered by the guide?
- (17) Are SCGs revised whenever necessary to promote effective derivative classification?
- (18) Are SCGs reviewed by the originator for currency and accuracy at least once every 5 years, or if concerning a defense acquisition program, prior to each acquisition program milestone, whichever occurs first?
- (19) Does the commander establish procedures through which authorized holders of classified information, within their commands, can challenge a classification decision, and make sure that command personnel are made aware of the established procedures?
- (20) Does each OCA:
- (a) Establish a system for processing, tracking, and recording formal challenges to classification?
  - (b) Provide an acknowledgment or written response to the challenge within 60 calendar days following the receipt of the challenge?
  - (c) Advise the challenger of the right to appeal the decision, if the challenge is denied and the OCA determines that the information is properly classified?
  - (d) Ensure information that is the subject of a classification challenge, continues to be classified and appropriately safeguarded until a decision is made to declassify it?
- f. Declassification, downgrading, upgrading, and destruction.*
- (1) Is information declassified when it no longer meets the standards and criteria for classification?
  - (2) Do commanders of ACOMs, ASCCs, and DRUs establish programs to make sure that records are reviewed and either declassified or exempted prior to the date for automatic declassification?
  - (3) Is declassification of RD and FRD information only with the express specific approval of the OCA for the information?

(4) Is information classified by other U.S. Executive Branch agencies, by foreign governments, or by international organizations (including foreign contractors) referred to the originating agency (or its successor in function) prior to declassification? (In the case of a foreign government, refer to its legitimate successor for a declassification decision.)

(5) Does the automatic declassification requirement exist for all records of permanent historical value as they become 25 years old?

(6) Are documents that are exempted from automatic declassification after 25 years, marked with the designation “25X” or 50X, followed by the number of the exemption category (see categories listed in paras 3–6c through 3–6f), or by a brief reference to the pertinent exemption?

(7) Do ACOMs, ASCCs, and DRUs that maintain physical custody/logistical control of federal records subject to the automatic declassification requirements of the EO:

(a) Report status of their reviews to ADA by completing the annual ADA LOC by 1 December of each year in accordance with this regulation?

(b) Ensure all personnel conducting automatic declassification reviews of records highly likely to contain RD are trained and certified by DOE by attending the Historical Records Restricted Data Reviewers Course?

(c) Provide a Proposal to Exempt Army Information memorandum to ADA for inclusion in the ADG (25X/50X) when proposing to exempt information not already specified in the ADG?

(8) Is information downgraded to a lower level of classification when the information no longer requires protection at the originally assigned level and can be properly protected?

(9) Is classified information upgraded to a higher level of classification only by officials who have been delegated the appropriate level of OCA? Do they also notify holders of the change in classification?

(10) Is classified material destroyed completely to preclude recognition or reconstruction of the classified information contained in or on the material? Is destruction accomplished in accordance with the guidelines outlined in this regulation?

*g. Controlled Unclassified Information.*

(1) Are unclassified documents and material containing CUI marked in accordance with DoDI 5200.48, as stated in this regulation?

(2) During working hours, are reasonable steps taken to minimize risk of access by unauthorized personnel?

(3) After working hours, is CUI stored in approved methods outlined in DoDI 5200.48?

(4) Are CUI documents and material transmitted by approved means?

(5) Is CUI destroyed properly as outlined in DoDI 5200.48?

*h. Access, control, safeguarding, and visits.*

(1) Prior to execution of SF 312, has the command verified security clearance eligibility of the individual in accordance with AR 380–67?

(2) Prior to granting access to classified information, do all DA personnel receive a briefing outlining their responsibility to protect classified information and have they signed the NDA?

(3) Are all DA personnel who are retiring, resigning, being discharged, or who will no longer have access to classified information, out-processed through the command’s security office or other designated command office, and are they formally debriefed?

(4) Are NDAs provided to the appropriate command personnel offices for filing in the individuals’ official personnel file/folders in accordance with chapter 5 of this regulation?

(5) Do commands maintain a system of control measures that ensures that access to classified information is limited only to authorized persons?

(6) Is classified material removed from storage kept under constant surveillance and control by authorized personnel?

(7) Are classified document cover sheets (SFs 703, 704, and 705) placed on classified documents when removed from storage?

(8) Do commands that access, process, or store classified information establish a system of security checks at the close of each working day to ensure that all classified material is properly secured?

(9) Is SF 701 used to record these checks?

(10) Have commands developed plans for the protection, removal, and destruction of classified material in case of fire, flood, earthquake, other natural disasters, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise?

(11) In telephone conversations, is classified information only discussed over STE and circuits approved for transmission of information at the level of classification being discussed?



(12) Are storage containers and IT equipment, which had been used to store or process classified information, inspected by cleared personnel before removal from protected areas or before unauthorized persons are allowed unescorted access to them?

(13) Have commands established procedures to control access to classified information by visitors?

(14) Does the command have security procedures that prescribe the appropriate safeguards to prevent unauthorized access to non-COMSEC-approved equipment, that are used to process classified information, and replace and destroy equipment parts, pursuant to the level of the classified material contained therein, when the information cannot be removed from them?

(15) Has the command developed procedures to protect incoming mail, bulk shipments, and items delivered by messenger, until a determination is made whether classified information is contained in the mail?

(16) Have screening points been established to limit access to classified information?

(17) Has the command established procedures to control all Secret and Confidential information and material originated, received, distributed, or routed to sub-elements within the command, and all information disposed of by the command by transfer of custody or destruction?

(18) Are working papers containing classified information handled in accordance with paragraph 5–20?

(19) Has the command established and enforced procedures for the reproduction of classified material which limit reproduction to that which is mission essential and do they make sure that appropriate countermeasures are taken to negate or minimize any risk?

(20) Are all copies of classified documents reproduced for any purpose, including those incorporated in working papers, subject to the same safeguards and controls prescribed for the document from which the reproduction is made?

(21) Is a written prohibition against unauthorized reproduction of information at any classification level prominently displayed?

(22) Is specific equipment designated for the reproduction of classified information and prominently marked as such?

(23) Have commands established procedures which ensure that appropriate approval is granted before classified material is reproduced?

(24) Are classified documents and other material retained only if they are required for effective and efficient operation of the command or if their retention is required by law or regulation?

(25) Do commanders ensure that the management of the retention of classified material is included in oversight and evaluation of program effectiveness?

(26) Are classified documents and materials destroyed by burning or, when meeting the standards contained in chapter 3 of this regulation, by melting, chemical decomposition, pulping, pulverizing, cross-cut shredding, or mutilation, sufficient to preclude recognition, or reconstruction of the classified information?

(27) Do the heads of DA commands, units, activities, agencies, and their subordinates establish and maintain a self-inspection program that includes periodic reviews and assessments, and annual assessments of their classified and CUI material?

*i. Storage and physical security standards.*

(1) Is classified information that is not under the personal control and observation of an authorized person guarded or stored in a locked security container, vault, room, or area pursuant to the level of classification and this regulation?

(2) Do commands establish administrative procedures for the control and accountability of keys and locks whenever key operated, high security padlocks are utilized?

(3) Is the requirement that there will be no external mark revealing the level of classified information authorized to be stored in a given container or vault being followed?

(4) Is the requirement that there will be no external mark revealing priorities for emergency evacuation and destruction marked or posted on the exterior of storage containers, vaults, or secure rooms followed?

(5) For identification and/or inventory purposes only, does each vault or container bear, externally, an assigned number or symbol?

(6) Are combinations changed?

(a) When the combination is placed in use?

(b) Whenever an individual knowing the combination no longer requires access?

(c) When the combination has been subject to possible compromise?

(d) When taken out of service, and are built-in combination locks reset to the standard combination in accordance with paragraph 6–8?

(7) Is the combination of a container, vault, or secure room used for the storage of classified information treated as information having a classification equal to the highest category of the classified information stored inside?

(8) Is a record maintained for each vault or secure room door, or container used for storage of classified information, using SF 700?

(9) Is access to the combination of a vault or container used for the storage of classified information granted only to those individuals who are authorized access to the classified information that is to be stored inside?

(10) Are entrances to secure rooms or areas either under visual control at all times during duty hours to preclude entry by unauthorized personnel, or are the entrances equipped with electric, mechanical, or electro-mechanical access control devices to limit access during duty hours?

(11) Have there been unapproved modifications or repairs to security containers and vault doors? (Considered a violation of the container's or door's integrity and the GSA label will be removed). If so, has the GSA label been removed?

(12) Have commands established procedures concerning repair and maintenance of classified material security containers, vaults, and secure rooms, to include a schedule for periodic maintenance?

(13) Is security equipment inspected before turn-in or transfer to ensure that classified material is not left in the container?

*j. Transmission and transportation.*

(1) Have commands established local procedures to meet the minimum requirements to minimize risk of compromise while permitting use of the most effective transmission or transportation means?

(2) Is Top Secret information transmitted only as outlined in paragraph 7-3?

(3) Is Secret information transmitted only as outlined in paragraph 7-4?

(4) Is Confidential information transmitted only as outlined in paragraph 7-5?

(5) Is classified information or material approved for release to a foreign government in accordance with AR 380-10?

(6) If required, is the material transferred only between authorized representatives of each government in compliance with the provisions of chapter 7 of this regulation?

(7) When classified material is hand-carried for delivery to a foreign government representative, or when classified information is discussed with or otherwise disclosed to foreign national personnel, are the requirements of AR 380-10 strictly followed?

(8) Where applicable, have commands established procedures for shipment of bulk classified material as freight, to include provisions for shipment in closed vehicles when required, appropriate notice to the consignee concerning the shipment, procedures at transshipment activities, and action to be taken in case of nondelivery or unexpected delay in delivery?

(9) When classified information is transferred, is it enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and to ease in detecting tampering, except where exempted by paragraph 7-8?

(10) Is the outer envelope or container for classified material addressed to an official government activity or to a DoD contractor with a facility clearance and appropriate storage capability?

(11) Does the inner envelope or container show the address of the receiving activity, the address of the sender, the highest classification of the contents, including, where appropriate, any special markings, and any other special instructions?

(12) Is the requirement that the outer envelope or single container not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified strictly followed?

(13) Is hand-carrying of classified material limited to situations of absolute necessity and carried out to make sure it does not pose an unacceptable risk to the information?

(14) Do responsible officials provide a written statement to all individuals escorting or carrying classified material authorizing such transmission?

(15) Do travelers who are authorized to carry classified material on international flights, or by surface conveyance if crossing international borders, have courier orders?

(16) Is the individual designated as courier in possession of a DoD or contractor-issued CAC that includes a photograph, descriptive data, and signature of the individual? (If the identification card does not contain date of birth, height, weight, and signature, these items must be included in the written authorization.)

*k. Security education and training.*

(1) Has the commander established a Security Education and Awareness Program?

(2) Have all DA personnel completed the initial security orientation, and annual training in accordance with chapter 8 of this regulation?

(3) Before being granted access to classified information, have all employees signed a SF 312?

- (4) Are DA personnel, who are in positions which require performance of specified roles in the Information Security Program, provided security education sufficient to permit quality performance of those duties?
- (5) Is the training provided before, concurrent with, or not later than 6 months following assumption of those positions, unless otherwise noted?
- (6) Are officials who have been granted OCA trained in their responsibilities before they exercise the delegated authority, and annually thereafter?
- (7) Has the OCA certified in writing that they received the training?
- (8) Are all DA personnel, whose responsibilities include derivative classification, trained in requirements and procedures appropriate to the information and material they will be classifying, to include the proper use of classification guides and source documents, and before exercising any derivative classifications?
- (9) Are SMs, security staff members, and others with significant responsibility for management of the Information Security Program trained and educated to fulfill their roles?
- (10) Are DA personnel that have been briefed on their responsibilities for protecting U.S. classified information, briefed simultaneously on the requirements for protecting NATO information?
- (11) Do commands include in their security education programs, either in the general program or as part of special briefings to select personnel affected, provisions regarding special education and training for personnel who:
  - (a) Use ISs to store, process, or transmit classified information?
  - (b) Will be traveling to foreign countries where special concerns about possible exploitation exist or will be attending professional meetings or conferences where foreign attendance is likely?
  - (c) Will be escorting, hand-carrying, or serving as a courier for classified material?
  - (d) Are authorized access to classified information requiring special control or safeguarding measures?
  - (e) Are involved with international programs?
- (12) Do commanders ensure that security education programs are appropriately evaluated during self-inspections and during oversight activities of subordinate commands or organizational units?
- (13) Do commands ensure that security education programs incorporate or provided separately training related to the protection, handling, and safeguarding of CUI?
- (14) Do commands maintain a record of the programs offered and of the personnel that participated? Are these records maintained for 2 years and available for review during oversight inspections and assistance visits?
  1. *Security incidents and reporting involving classified information.*
    - (1) Are personnel aware of their responsibilities in the event of an actual or possible compromise or loss of classified information or material?
    - (2) When an incident of possible loss or compromise of classified information is reported, does the command immediately initiate an inquiry into the incident?
    - (3) Does the person appointed to conduct the inquiry have the appropriate security clearance, the ability and available resources to conduct an effective inquiry, and is not likely to have been involved, directly or indirectly, in the incident?
    - (4) In cases of apparent loss of classified material, has the person conducting the inquiry ensured that a thorough search for the material has been conducted, and has documented the steps taken to locate the material?
    - (5) Does the inquiry sufficiently answer the questions outlined in DoDM 5200.01, Volume 3?
    - (6) If at any time during the inquiry, it appears that deliberate compromise of classified information may have occurred, has the situation been immediately reported to the chain of command and supporting CI unit?
    - (7) Have apparent violations of other criminal law been reported to the supporting criminal investigative activity? When notified of possible or actual compromise, has the holder of that information or material ensured that the OCA responsible for each item of information, was notified of the incident?
    - (8) If classified information appears in the public media, including public internet sites, or if approached by a representative of the media or other individual, are personnel briefed on not making any statement or comment that confirms the accuracy of or verifies the classified status of the information, and to report the contact immediately to the appropriate command security and public affairs authorities?
    - (9) In cases where a person has had unauthorized access to classified information, has the person been debriefed to enhance the probability that they will properly protect it?
    - (10) Have commanders of ACOMs, ASCCs, and DRUs established necessary reporting and oversight mechanisms to make sure that inquiries are conducted, when required, that they are done in a timely and effective manner, and that appropriate management action is taken to correct identified problem areas?
    - (11) Have commanders of ACOMs, ASCCs, and DRUs established a system of controls and procedures to make sure that reports of security inquiries and damage assessments are conducted, when required, and that their results are available as needed?

(12) When an individual who has had access to classified information is absent without authorization, commits or attempts to commit suicide, or is temporarily or permanently incapacitated, has the command inquired into the situation to see if there are indications of activities, behavior, or associations that could indicate classified information might be at risk?

**B-5. Comments**

Help make this a better tool for evaluating internal controls. Submit comments to the DCS, G-2 (DAMI-CDS), [usarmy.pentagon.hqda-dcs-g-2.mbx.security-message@mail.mil](mailto:usarmy.pentagon.hqda-dcs-g-2.mbx.security-message@mail.mil).

**B-6. Supersession**

This evaluation replaces the checklist previously published in AR 380-5, dated 22 October 2019.

## **Glossary**

### **Section I**

#### **Abbreviations**

**AASA**

Administrative Assistant to the Secretary of the Army

**ACOM**

Army command

**ADA**

Army Declassification Activity

**ADG**

Army Declassification Guide

**AECS**

Automated Entry Control System

**ALMS**

Army Learning Management System

**AR**

Army regulation

**ARIMS**

Army Records Information Management System

**ASCC**

Army service component command

**B&P**

bid and proposal

**CAC**

common access card

**CDSE**

Center for Development of Security Excellence

**CFR**

Code of Federal Regulations

**CI**

counterintelligence

**CID**

Criminal Investigation Command

**CNWDI**

critical nuclear weapons design information

**COMSEC**

communications security

**CPI**

critical program information

**CSS**

Central Security Service

**CUI**

Controlled Unclassified Information

**DA**

Department of the Army

**DA Form**

Department of the Army form

**DCD**

Defense Courier Division

**DCS**

Deputy Chief of Staff

**DCSA**

Defense Counterintelligence and Security Agency

**DD Form**

Department of Defense form

**DISS**

Defense Information System for Security

**DNI**

Director of National Intelligence

**DoD**

Department of Defense

**DoDD**

Department of Defense directive

**DoDI**

Department of Defense instruction

**DoDM**

Department of Defense manual

**DOE**

U.S. Department of Energy

**DRU**

direct reporting unit

**DTIC**

Defense Technical Information Center

**EO**

Executive Order

**EPL**

evaluated products list

**FED-STD**

federal standard

**FGI**

foreign government information

**FOIA**

Freedom of Information Act

**FRD**

Formerly Restricted Data

**FSE**

file series exemption

**GAO**

Government Accountability Office

**GPO**

Government Publishing Office

**GS**

general schedule

**GSA**

General Services Administration

**HQDA**

Headquarters, Department of the Army

**IDE**

intrusion detection equipment

**IDS**

intrusion detection system

**IR&D**

independent research and development

**IS**

information system

**ISCAP**

Interagency Security Classification Appeals Panel

**ISOO**

Information Security Oversight Office

**IT**

information technology

**LOC**

letter of certification

**MDR**

mandatory declassification review

**MIL–HDBK**

military handbook

**NATO**

North Atlantic Treaty Organization

**NDA**

nondisclosure agreement

**NIPRNET**

nonclassified internet protocol router network

**NSA**

National Security Agency

**OCA**

original classification authority

**OPF**

official personnel folder

**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

**PIN**

personal identification number

**RD**

Restricted Data

**SAP**

special access program

**SCG**

security classification guide

**SCI**

sensitive compartmented information

**SECARMY**

Secretary of the Army

**SF**

standard form

**SIPRNET**

secure internet protocol router network

**SM**

security manager

**SPM**

special program manager

**STE**

secure terminal equipment

**TSA**

Transportation Security Administration

**TSCM**

technical security countermeasures

**TSCO**

Top Secret control officer

**UL**

Underwriters Laboratories

**USC**

United States Code

**USPS**

United States Postal Service

**USSAN**

United States Security Authority for North Atlantic Treaty Organization

**WMD**

weapon of mass destruction

**Section II****Terms****Access**

The ability or opportunity to obtain knowledge of classified information.

**Agency**

In addition to the DoDM 5200.01, Volume 1 definition, this term also includes the Army (an ACOM is not an agency, but rather is part of an agency, the Army). Within DoD, this term includes the DoD, DA, the Department of the Navy, and the Department of the Air Force.



**Authorized person**

Defined in DoDM 5200.01, Volume 1.

**Automatic declassification**

Defined in DoDM 5200.01, Volume 1

**Carve-out**

Defined in DoDM 5220.02, Volume 1.

**Classification**

Defined in DoDM 5200.01, Volume 1.

**Classification guidance**

Defined in DoDM 5200.01, Volume 1.

**Classification guide**

Defined in DoDM 5200.01, Volume 1.

**Classified national security information (or “classified information”)**

Defined in DoDM 5200.01, Volume 1.

**Classifier**

Defined in DoDM 5200.01, Volume 1.

**Code word**

A single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans or operations classified as Confidential or higher.

**Collateral information**

Defined in DoDM 5200.01, Volume 1.

**Command**

HQDA to include the Office of the SECARMY and the Army Staff, ACOMs, ASCCs, DRUs, major subordinate commands and other organizations formed within the Army to support HQDA or an ACOM, ASCC, or DRU.

**Common access card**

An identification card displaying the cardholder’s name, photo, and organization. The CAC is the DoD implementation of Homeland Security Presidential Directive 12 that requires federal executive departments and agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors, for access to federal facilities and ISs and designates the major milestones for implementation.

**Communications security**

Defined in DoDM 5200.01, Volume 1.

**Compilation**

Defined in DoDM 5200.01, Volume 1.

**Compromise**

An unauthorized disclosure of classified information.

**Confidential**

Defined in DoDM 5200.01, Volume 1.

**Continental United States**

U.S. territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

**Controlled cryptographic item**

A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but controlled. (Equipment and components so designated bear the designator “Controlled Cryptographic Item” or “CCI.”)

**Controlled Unclassified Information**

Defined in 32 CFR 2002.4.

**Counterintelligence**

Those activities which are concerned with identifying and counteracting the threat to security (of the Army and U.S. Government to include, but not limited to, its technology or industrial base) posed by foreign intelligence services or organizations, or by individuals engaged in espionage, sabotage, sedition, subversion, or terrorism.

**Critical nuclear weapon design information**

Defined in DoDM 5200.01, Volume 2.

**Damage assessment**

Defined in DoDM 5200.01, Volume 3.

**Damage to the national security**

Defined in DoDM 5200.01, Volume 3.

**Declassification**

Defined in DoDM 5200.01, Volume 1.

**Declassification authority**

Defined in DoDM 5200.01, Volume 3.

**Declassification guide**

Defined in DoDM 5200.01, Volume 3.

**Department of Defense component**

Defined in DoDM 5200.01, Volume 1.

**Department of the Army personnel**

Includes Regular Army, U.S. Army Reserve, or Army National Guard/Army National Guard of the United States military personnel assigned or attached to a DA installation or activity and civilian persons employed by, assigned to, or acting for an activity within DA.

**Derivative classification**

Defined in DoDM 5200.01, Volume 3.

**Document**

Defined in DoDM 5200.01, Volume 3.

**Downgrading**

Defined in DoDM 5200.01, Volume 3.

**Escort**

Defined in DoDM 5200.01, Volume 3.

**Event**

An occurrence or happening that is reasonably certain to occur, and which can be set as the signal for automatic declassification of information.

**Exception**

Defined in DoDM 5200.01, Volume 1.

**File series**

Defined in DoDM 5200.01, Volume 1.

**Foreign government information**

Defined in DoDM 5200.01, Volume 3.

**Foreign government representative**

For the purposes of this regulation, foreign nationals or U.S. citizens or nationals who are acting as representatives of either a foreign government or a firm or person sponsored by a foreign government. These individuals may interact officially with DA elements only in support of an actual or potential U.S. Government program (for example, Foreign Military Sales, U.S. government contract, or international agreement).

**Foreign nationals**

A person who is not a citizen or national of the United States or its territories. This definition does not include permanent residents (formerly immigrant aliens, resident aliens, or intending U.S. citizens). For the purposes of this regulation, a private non-U.S. citizen or national having no official affiliation with their government of origin. See definition of foreign government representative.

**Formerly Restricted Data**

Defined in DoDM 5200.01, Volume 3.

**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**

Defined in DoDM 5200.01, Volume 1.

**Information system**

An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

**Infraction**

Defined in DoDM 5200.01, Volume 3.

**Inquiry**

Defined in DoDM 5200.01, Volume 3.

**Integrity**

Defined in DoDM 5200.01, Volume 3.

**Intelligence activity**

An activity that an agency within the intelligence community is authorized to conduct under EO 12333.

**Investigation**

Defined in DoDM 5200.01, Volume 3.

**Legacy material**

Defined in 32 CFR 2002.4.

**Loss**

The inability to physically locate or account for classified information.

**Mandatory declassification review**

Review for declassification of classified information in response to a request for declassification that meets the requirements under EO 13526, Section 3.5.

**Material**

Defined in DoDM 5200.01, Volume 1.

**National security**

Defined in DoDM 5200.01, Volume 1.

**Need-to-know**

Defined in DoDM 5200.01, Volume 3.

**Network**

Defined in DoDM 5200.01, Volume 3.

**Nickname**

Defined in DoDM 5200.01, Volume 3.

**Open storage**

An area constructed in accordance with this regulation and authorized by the commander or other official where so designated for open storage of classified information.

**Operations security**

The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conducting of military operations and other activities.

**Original classification**

Defined in DoDM 5200.01, Volume 1.

**Original classification authority**

In addition to the DoDM 5200.01, Volume 3 definition, this term also includes: An individual's position, which has been authorized in writing, either by the President, SECARMY, or the DCS, G-2, to originally classify information up to and including a certain classification level.

**Permanent historical value**

In addition to the DoDM 5200.01, Volume 3 definition, this term also includes: Those records that have been identified in an agency records schedule as being permanently valuable. For Army records, see AR 25-400-2.

**Personal identifier**

Any grouping of letters or numbers, used in an organization code, that the command uses to identify a position.

**Personally identifiable information**

Defined in DoDM 5200.01, Volume 3.

**Restricted Data**

Defined in DoDM 5200.01, Volume 3.

**Safeguarding**

Defined in DoDM 5200.01, Volume 3.

**Secret**

Defined in DoDM 5200.01, Volume 1.

**Secure room**

Defined in DoDM 5200.01, Volume 3 (see open storage definition).

**Security classification guide**

Defined in DoDM 5200.01, Volume 1.

**Security clearance**

Defined in DoDM 5200.01, Volume 1.

**Security educator**

Person(s) responsible for providing security training as outlined in chapter 8 of this regulation.

**Security-in-depth**

In addition to the DoDM 5200.01, Volume 3 definition, this term also includes: A determination by the commander or other official where so designated, 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 especially during nonworking hours, closed-circuit video monitoring, or other safeguards that mitigate the vulnerability of unalarmed open storage areas and security containers during nonworking hours.

**Self-inspection**

Defined in DoDM 5200.01, Volume 3.

**Senior agency official**

In addition to the DoDM 5200.01, Volume 3 definition, this term also includes: Within DA, the SECARMY has appointed the DCS, G-2, as the Senior Agency Official.

**Sensitive compartmented information facility**

Defined in DoDM 5105.21.

**Sensitive information**

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 USC 552a (Privacy Act), but which has not been specifically authorized under criteria established by an EO or an Act of Congress to be kept Secret in the interest of national defense or foreign policy.

**Source document**

An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

**Special access program**

Defined in DoDM 5200.01, Volume 1.

**Systematic declassification review**

The review process for declassification of classified information contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with 44 USC Chapter 33.

**Technical counterintelligence (TEMPEST) countermeasures**

Any action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment or facility that electronically processes information for technical exploitation of classified and/or sensitive information.

**Telecommunications**

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

**TEMPEST**

A short name referring to the evaluation and control of compromising emanations from telecommunications and automated ISs equipment. TEMPEST countermeasures are designed to prevent Foreign Intelligence Service exploitation of compromising emanations by containing them within the IS of the equipment or facility processing classified information.

**Top Secret**

Defined in DoDM 5200.01, Volume 1.

**Unauthorized disclosure**

Defined in DoDM 5200.01, Volume 1.

**Upgrade**

To raise the classification of an item of information from one level to a higher one.

**Violation**

Defined in DoDM 5200.01, Volume 3.

**Waiver**

Defined in DoDM 5200.01, Volume 1.

**UNCLASSIFIED**

**PIN 004067-000**