

Army Regulation 380–28

Security

**Army Sensitive
Compartmented
Information
Security
Program**

**Headquarters
Department of the Army
Washington, DC
13 August 2018**

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–28

Army Sensitive Compartmented Information Security Program

This is a major revision, dated 13 August 2018—

- o Changes the title of the regulation from “Department of the Army Special Security System” to “Army Sensitive Compartmented Information Security Program” (cover).
- o Updates language related to the Deputy Chief of Staff, G–2 as the Head of the Intelligence Community Element (para 2–1).
- o Updates the roles and responsibilities of commanders of Army commands, Army service component commands, direct reporting units, and others with a sensitive compartmented information mission requirement (paras 2–3 through 2–10).
- o Establishes commanders of Army commands, Army service component commands, direct reporting units, and the Chief, National Guard Bureau as senior sensitive compartmented information security officials with requirements to establish a command level special security program (para 2–3).
- o Removes the Sensitive Compartmented Information Nondisclosure Statement and replaces it with the Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement) and provides parameters for the Government and the individual’s obligations (para 3–5).
- o Provides policy for the Entry-Exit Inspection Program (para 6–6*h*).
- o Adds policy for portable electronic devices and other prohibited items (chap 7).
- o Adds policy for the Security Education, Training, and Awareness Program (chap 9).
- o Adds policy for the Army's automated Sensitive Compartmented Information Security Program management tool (para 10–3).
- o Updates sensitive compartmented information access for the executive, legislative, and judicial branches (chap 12).
- o Adds an Internal Control Evaluation (see app B).

Security

Army Sensitive Compartmented Information Security Program

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official: 

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

History. This publication is a major revision.

Summary. This regulation establishes policy, procedures, and responsibilities for the Sensitive Compartmented Information Security Program. It implements National Policy, Intelligence Community Policy Guidance, Intelligence Community Standards and Intelligence Community Directives for the direction, administration, and management of Special Security Programs; and Department of Defense security policy as promulgated in DODM 5105.21, Volumes 1 through 3 and DODM 5200.1, Volumes 1 through 4.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserves, unless otherwise stated. It also applies to Department of the Army civilian personnel and Army contractors authorized to receive, store, process, or use sensitive compartmented information.

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 or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating 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 guidance.

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 appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Headquarters, Department of the Army (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Distribution. This publication 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, page 1

Purpose • 1–1, page 1

References • 1–2, page 1

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

Responsibilities • 1–4, page 1

Waivers • 1–5, page 1

Chapter 2

Responsibilities, page 1

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

Commanding General, U.S. Army Training and Doctrine Command • 2–2, page 2

Commanders of Army commands, Army service component commands, direct reporting units, and Chief, National Guard Bureau • 2–3, page 2

Senior intelligence officers of Army commands, Army service component commands, direct reporting units, and Chief, National Guard Bureau • 2–4, page 3

*This regulation supersedes AR 380-28, dated 1 September 1991.

Contents—Continued

Subordinate command senior intelligence officials • 2–5, *page 3*
Special security officer • 2–6, *page 4*
Contract special security officer • 2–7, *page 5*
Special security representative • 2–8, *page 5*
Sensitive compartmented information contract monitor • 2–9, *page 5*
Sensitive compartmented information indoctrinated personnel • 2–10, *page 5*

Chapter 3

Sensitive Compartmented Information Personnel Security, *page 6*

General • 3–1, *page 6*
Approval authority • 3–2, *page 6*
Requirements for sensitive compartmented information access • 3–3, *page 6*
Sensitive compartmented information access management • 3–4, *page 7*
Sensitive compartmented information indoctrination • 3–5, *page 7*
Special circumstances • 3–6, *page 8*
Suspension, debriefing, or revocation of sensitive compartmented information access • 3–7, *page 8*
Reciprocity of accesses (transfer-in-status) individuals • 3–8, *page 9*
Tier 5 Reinvestigation procedures • 3–9, *page 10*
Change in personal status • 3–10, *page 10*
Employee outside activities • 3–11, *page 10*
Personnel security files • 3–12, *page 11*
Security prepublication review process • 3–13, *page 11*
Contact with foreign nationals • 3–14, *page 11*
Foreign travel • 3–15, *page 12*

Chapter 4

Sensitive Compartmented Information Security, *page 13*

Individuals • 4–1, *page 13*
Contractors • 4–2, *page 13*
Courier authorizations and requirements • 4–3, *page 13*
DD Form 2501 • 4–4, *page 13*
Marking requirements • 4–5, *page 14*

Chapter 5

Security Incidents, *page 14*

Security incidents • 5–1, *page 14*
Inquiries and investigations • 5–2, *page 14*
Corrective action • 5–3, *page 15*
Classification review • 5–4, *page 15*
Damage assessments • 5–5, *page 15*
Case file retention • 5–6, *page 16*
Inadvertent sensitive compartmented information disclosure agreement • 5–7, *page 16*
Damaged Defense Courier Service packages • 5–8, *page 16*
Reporting missing sensitive compartmented information -indoctrinated personnel • 5–9, *page 16*
Reporting procedures • 5–10, *page 16*
Reporting/responding to classified information appearing in the public domain or media • 5–11, *page 17*

Chapter 6

Physical Security, *page 17*

Sensitive compartmented information physical security • 6–1, *page 17*
Concept approval for establishing a permanent sensitive compartmented information facility • 6–2, *page 17*
Temporary sensitive compartmented information facilities • 6–3, *page 18*
Temporary secure working area • 6–4, *page 18*
General • 6–5, *page 18*
Inspection policy • 6–6, *page 18*

Contents—Continued

Chapter 7

Portable Electronic Devices and Other Prohibited Items, *page 19*

Personally owned portable electronic devices, including personal wearable fitness devices • 7–1, *page 19*

Restrictions • 7–2, *page 19*

Misuse or violation of portable electronic device policy • 7–3, *page 19*

Additional prohibited items in a sensitive compartmented information facility • 7–4, *page 20*

Exceptions • 7–5, *page 20*

Waivers • 7–6, *page 20*

Chapter 8

Sensitive Compartmented Information Industrial Security Program, *page 20*

Appointment of sensitive compartmented information contract monitors • 8–1, *page 20*

Contractor and Government sensitive compartmented information facilities • 8–2, *page 21*

Chapter 9

Sensitive Compartmented Information Security Education, Training, and Awareness Program, *page 21*

Requirements for sensitive compartmented information security officials • 9–1, *page 21*

Sensitive Compartmented Information indoctrination and initial security orientation • 9–2, *page 21*

Sensitive Compartmented Information Security Awareness Program • 9–3, *page 21*

Continuing security annual refresher training and education and awareness • 9–4, *page 22*

Chapter 10

General Administration, *page 22*

Standard operating procedures • 10–1, *page 22*

Defense Intelligence Agency Compartmented Address Book • 10–2, *page 22*

Army's Automated Sensitive Compartmented Information Security Program Management System • 10–3, *page 22*

Chapter 11

Visitor Control, *page 22*

Visitor control • 11–1, *page 22*

Foreign national visits or sensitive compartmented information facility access • 11–2, *page 23*

Chapter 12

Sensitive Compartmented Information Facility Access for the Executive, Legislative, and Judicial Branches, *page 23*

Executive branch access • 12–1, *page 23*

Legislative branch access • 12–2, *page 23*

Judicial branch access • 12–3, *page 23*

Appendixes

A. References, *page 24*

B. Internal Control Evaluation Checklist, *page 29*

Glossary

Chapter 1

General

1–1. Purpose

This regulation establishes policy and assigns responsibilities for the management, protection, use, and dissemination of sensitive compartmented information (SCI) within the Department of the Army (DA) as directed by the Director of National Intelligence (DNI), the Under Secretary of Defense for Intelligence (USD(I)), and the Defense Special Security System. Policy promulgated herein implements executive orders (EO), Office of the Director of National Intelligence Directives, Department of Defense (DOD) issuances, Army regulations, and other documents cited for guidance on the management of a command SCI Security Program. This regulation implements a risk management philosophy that empowers commanders, senior intelligence officers (SIOs) and their security staff to make decisions based on the threat, appropriate countermeasures, and resources available. AR 380–381 and DODM 5205.07 V–3 govern the security of Special Access Program (SAP) information within a sensitive compartmented information facility (SCIF). AR 380–49, DOD 5220.22–R, DOD 5220.22–M, DOD 5220.22–M-Sup 1, and DODM 5105.21, V 1–3, govern access, and release of SCI to Army contractors. Authorities and responsibilities for the Army SCI Security Program are derived from the DNI, and through the USD(I) and the Defense Intelligence Agency (DIA) to the Deputy Chief of Staff (DCS), G–2, as the Head of the Intelligence Community Element (HICE) for the Army and implemented by the Special Security Office (SSO) Army in accordance with DODM 5105.21, V–1.

1–2. References

See appendix A.

1–3. Explanation of abbreviations and terms

See the glossary.

1–4. Responsibilities

Responsibilities are listed in chapter 2.

1–5. Waivers

The DCS, G–2 reviews and may approve requests for exceptions (deviations, waivers, or contingencies) to this regulation, as appropriate and as consistent with law and policy. Army commands (ACOMs), Army service component commands (ASCCs), direct reporting units (DRUs), Army National Guard (ARNG), and other Army organizations with SCI missions will submit such requests with justification to the Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Chapter 2

Responsibilities

2–1. Deputy Chief of Staff, G–2

In accordance with DODM 5105.21, V–1, as the Head of the Intelligence Community Element for the Army, the DCS, G–2 will—

- a.* Administer, oversee, and execute the SCI Security Program and SSO System for the Army, in accordance with policies established by the DIA, as the DOD proponent for SCI policy.
- b.* Assist the Director, DIA in developing and recommending appropriate SCI security policy by appointing a knowledgeable SCI security policy representative to the SCI Policy Coordination Committee.
- c.* Conduct a continuing review of the Army’s SCI Security Program including oversight of the Army’s SCI Security Program. Review and evaluation of subordinate SCI Security Programs will include staff assistance visits (SAVs) or assessments to ensure compliance with security policies, including ensuring a continuing security education, training, and awareness program to annually educate SCI security officials and personnel with SCI access is conducted at all levels.
- d.* Ensure effective training is available for Army SCI security officials.
- e.* Establish procedures to ensure security violations and unauthorized disclosures of SCI are properly investigated and reported.

f. Ensure SSO-related resources are provided, and promulgate resource management guidance to commands for the proper administration of SCI Security Programs within the Army.

g. Approve the establishment of any permanent SCIF, temporary SCIF (T-SCIF) and temporary secure working area (TSWA). This approval authority may be delegated to the SIO at the ACOMs, ASCCs, DRUs, and ARNG Headquarters. This approval authority will not be further delegated.

h. Designate the director of HQDA, Office of the Deputy Chief of Staff (ODCS), G-2, Counterintelligence, Human Source Intelligence (HUMINT), Disclosure and Security Directorate (DAMI-CDS) to act as the cognizant security authority concerning the Army Security Program management and oversight for all matters related to the protection of intelligence sources and methods and for implementation of the Army's SCI program.

i. The cognizant security authority will, as delegated by the DCS, G-2, have authority over and responsibility for all aspects of management and oversight of the security program established for the protection of intelligence sources and methods, and for implementation of SCI security policy and procedures defined in DOD and DNI policies for the Army SCI Security Program.

j. Direct the HQDA, SSO (SSO Army) to execute the Army's SCI Security Program.

k. Direct the Commanding General (CG), U.S. Army Intelligence and Security Command (INSCOM) to oversee, manage, and implement the Army SCI Industrial Security Program pursuant to AR 380-49.

l. Review and approve as appropriate the "need-to-know" requests for access to SCI. This authority may be delegated to Commanders of ACOMs, ASCCs, DRUs, and the Chief, NGB (who may further delegate such authority to the Director, ARNG) for approval of access to SCI for personnel under their security cognizance.

m. The CG, INSCOM will—

(1) Provide dedicated, centralized support, program management, and oversight to Army SCI contracts and contractor personnel.

(2) Establish and maintain the automated central SCI database, Army Centralized Contracts and Security Portal (ACCS), and approved follow-on system for Army SCI contractors to include information related to all Army SCI contracts, SCI contract monitors, contractor companies, and facilities.

(3) Establish, execute, and manage an Army SCI Program for the oversight and management of DA affiliated contracts and contractors. Ensure SAVs are conducted at least biannually.

(4) Establish, execute, and manage the Army SCI Program for the oversight of DA affiliated contractors, including ensuring all contracts are valid (validate cage code and top secret (TS) facility clearance and monitor all contract terminations, as well as managing, monitoring, coordinating, and finalizing the investigation and reporting of SCI security violations for contractors).

(5) Appoint all primary and alternate SCI security officials such as contractor special security officer (CSSO), talent keyhole control officer, gamma control officer, and HUMINT control systems special control officer, if applicable.

(6) Ensure all prime and sub-contracted SCI-access certification information on DD Form 254 (Department of Defense Contract Security Specification) are entered and processed in ACCS or approved follow-on system.

(7) Review DD Form 254 and DA SCI addendum for contracts requiring SCI for completion and accuracy prior to contracting.

(8) Forward unfavorable security actions concerning contract personnel – statement of reasons, incident reports, requests for information, psychological evaluations, and drug and alcohol evaluations to the Department of Defense Consolidated Adjudication Facility (DOD CAF).

(9) Review, approve, and coordinate contractor SCIF concept proposals, standard operating procedures (SOPs), T-SCIF, TSWA, and Emergency Action Plans.

2-2. Commanding General, U.S. Army Training and Doctrine Command

The CG, TRADOC will—

a. Establish and publish SCI/SSO doctrinal literature for all Army organizations.

b. Ensure SCI management is integrated into the functions and training into combat development, operational and intelligence doctrine, and training of the force.

c. Develop and publish approved SCI/SSO operational concepts which describe capabilities required for employing Army forces in the future and that provide the basis for changes in doctrine, organization, training, materiel, and leader and education – personnel, facilities, and policy.

2-3. Commanders of Army commands, Army service component commands, direct reporting units, and Chief, National Guard Bureau

Commanders of ACOMs, ASCCs, DRUs, and Chief, NGB will—

- a. Establish SCI programs that will provide management, oversight, and implementation of SCI security policy and procedures within their command and subordinate organizations.
- b. Designate an SIO, in writing.
- c. Approve the need-to-know for access to SCI for personnel under their security cognizance.

2–4. Senior intelligence officers of Army commands, Army service component commands, direct reporting units, and Chief, National Guard Bureau

The SIO will be the senior-most commissioned or warrant officer or DA Civilian in an intelligence career field and appointed in writing by an organization commander to oversee and manage intelligence and security functions within the organization. Every commander whose organization is involved with SCI must appoint an SIO, or act as the SIO. The SIO must have a final TS/SCI clearance without exceptions. The responsibilities of the ACOM, ASCC, DRU, and ARNG SIO may not be further delegated. The SIO will—

- a. Implement organizational intelligence and SCI security functions in accordance with this regulation and DODM 5105.21, V–1, Enclosure 3, as well as all other applicable regulations and guidance.
- b. Exercise overall management of the command’s SCI program and is responsible for the oversight and execution of all SCI related functions, including administering the SCI program, oversight for subordinate SCI operations, ensuring organizational SCI programs adhere to applicable security policies and procedures. Evaluate SCI management programs of subordinate organizations by including SCI functional areas within the command’s organizational inspection program in accordance with AR 1–201.
- c. Ensure adequate resources to accomplish the SCI management mission within the organization are programmed within the Programming Process Budget Execution System and resourced, including resources for establishing new SCI facilities with concept approvals.
- d. Ensure SCI functions are integrated into command and subordinate command contingency plans.
- e. Employ SCI functions during exercises and major deployments in conformity with wartime standards and evaluate as a part of a unit’s ability to deploy effectively.
- f. Ensure that SSOs and assistant SSOs (ASSOs) are trained to perform their duties and attend the DOD SCI Security Officials Course or a similar course from the list maintained by SSO Army within 180 days of appointment.
- g. Ensure that security violations and unauthorized disclosures of SCI or other information that could impact on an individual’s continued eligibility for access to SCI are properly reported in accordance with AR 380–67 and DODM 5105.21, V–3, Enclosure 5.
- h. Ensure subordinate commands submit their annual SCI access report. The report will be consolidated at the ACOM, ASCC, and DRU levels and forwarded to Headquarters, Department of the Army (HQDA) SSO no later than 1 November annually. The report will include SCI accesses by category and total number of personnel briefed as of 30 September annually.
- i. Ensure subordinate commands conduct annual SCIF self-inspections. Identify deficiencies and document corrective actions collectively and forward consolidated results to HQDA SSO no later than 31 October of the year.
- j. Establish and implement approval and monitoring procedures for T–SCIF and TSWA.
- k. Approve T–SCIFs for a period not to exceed 1 year. T–SCIFs that require operation beyond the 1-year period may be justified in writing to the DIA, SCIF Management Branch, which retains approval authority for extensions.
- l. Establish a security oversight program for T–SCIF SCI operations to ensure subordinate organizations are in compliance with SCI regulatory policies and procedures.
- m. Develop implementation guidance that adheres to information assurance policies and procedures regarding the use of removable and rewritable media and information systems with subordinate SCIFs.
- n. Appoint a fully qualified SSO, in writing. In the absence of an appointed SSO, the SIO will act as the SSO. A copy of appointment orders will be retained in the command’s official records.

2–5. Subordinate command senior intelligence officials

The SIO at commands subordinate to the ACOMs, ASCCs, DRUs, and headquarters ARNG must have a final TS/SCI clearance without waivers and will—

- a. Be responsible for the command’s SCI Security Program. The SIO will appoint an SSO in writing to directly support the SIO and all primary and alternate SSOs, special security representatives (SSRs), information assurance (IA) managers, IA officers, and control officers as required for all authorized SCI compartments. In the absence of an appointed SSO, the SIO will act as the SSO.
- b. The command SSO will be functionally subordinate to the SIO and be a member of the SIO staff. The command SSO will be responsible for a command’s SCIFs, provide direct support to other SSOs, SSRs, or contractor SSOs and have direct access to the SIO.

- c. Provide proper protection, use, and dissemination of SCI documents and material by enforcing SCI, information, personnel, physical, communications, industrial, and IA security rules and by developing SOPs and practices.
- d. Maintain the integrity of the SCI control system. SSO and CSSO personnel will not perform duties or details that conflict or interfere with their SCI security responsibilities or with the security of SCI.
- e. Approve or validate the need-to-know for individuals (military, civilian Government employee, or contractor) requiring SCI access and validate the need to establish SCIFs, SCI communications, and information system.
- f. Identify required communications electronics and communications security equipment to local supporting communications elements. Establish a memorandum of agreement with the supporting communications element to provide timely communications support to the intelligence mission, if necessary.
- g. Establish memorandum of agreements with other organizations, as necessary, to address SCI areas of responsibility, training, operational needs, support, and services. Implement SOPs, as required, for further definition and clarification of security responsibilities.
- h. Establish a co-utilization agreement between the SSO and the local program security officer for any SAP operating in the SCIF and monitor compliance with the co-utilization agreement.
- i. Train SSOs and SSRs to perform their duties and meet responsibilities.
- j. Provide sufficient qualified personnel, funds, work space, facilities, and logistical support to effectively operate the SCI Security Program.
- k. Evaluate and send to the Defense Messaging System requests to use the Defense Special Security Communication System for SAPs and other special programs or projects.
- l. Request that DOD counterparts responsible for military police activities direct subordinate military police activities to provide SSOs all derogatory information on SCI-indoctrinated personnel.
- m. Keep the SSO informed of issues having SCI implications such as facilities utilization, information system requirements, base security, or base or post resource protection.
- n. Designate SCI couriers for hand-carrying SCI outside the United States. The SIO may delegate this authority to the SSO except for couriering aboard foreign-flag aircraft.

2–6. Special security officer

The special security officer (SSO) is a commissioned officer, warrant officer, noncommissioned officer (E–7 or above) or DA Civilian (general schedule (GS)-9 or above), who manages the SCI Security Program and oversees SCI security functions for U.S. Government SCIFs in accordance with DODM 5105.21, V–1, Enclosure 2. Assignment as the SSO is a primary duty and SSOs will not be assigned duties or details that conflict or interfere with performance of SCI control responsibilities. Assignment of an SSO in G–2, or command security office position does not constitute a conflict of interest. The SSO must have a final TS/SCI clearance without waivers. The SSO will—

- a. Ensure appropriate accreditation documentation is available for each SCIF and communications/information systems under the organization’s security cognizance.
- b. Maintain a copy of appointment orders on file for him or herself and all subordinate SSRs.
- c. Attend DNI- or DIA-sponsored SSO refresher training every 4 years following required initial training, from a list of approved training maintained by the SSO Army.
- d. Manage all actions related to SCI personnel, information, physical, and technical security (telecommunications electronics materiel protected from emanating spurious transmissions (TEMPEST)/technical surveillance countermeasures (TSCM)) procedures according to this and all current regulations.
- e. Serve as the official channel for certifying and receiving SCI visitor clearances/accesses.
- f. Manage personnel security functions such as conducting security briefings, indoctrinations, and debriefings, and executing nondisclosure agreements for all SCI personnel, as well as providing oversight and support to SAPs within the SCIF in accordance with AR 380–381.
- g. Ensure that all SCI-indoctrinated personnel (whether Soldier, DA Civilian or contractor), upon separation from employment, transfer in status, or retirement which requires a debriefing, sign and forward written agreement to report all employment with foreign government entities for 2 years starting on the date of separation and to further report any change in status of employment with foreign government entities, in accordance with AR 600–291.
- h. Ensure annual self-inspections are conducted by all SCI security officials, conduct oversight reviews and forward the results to the next-higher echelon SSO, retaining copies in records for 1 year or until the next self-inspection.
- i. Conduct required annual training for all SCI personnel.
- j. Ensure all SCI personnel are informed of current policies concerning the use of wireless technology in SCIFs.
- k. Immediately report any and all known and suspected security violations to the SIO, information assurance officer, and to counterintelligence authorities as appropriate in accordance with AR 380–5. Prepare required reports, in accordance with DODM 5105.21, V–1, Enclosure 5 and current Army regulations.

- l.* Manage and supervise SCI access, and provide support to contractors operating in an Army SCIF, including establishing and using an account on the ACCS System.
- m.* Utilize SSO automation systems provided by the Army, including all available modules.

2-7. Contract special security officer

The CSSO is a contractor, who manages the SCI Security Program and oversees SCI security functions for a contractor's SCIF in accordance with DODM 5105.21, V-1, Enclosure 2. The CSSO must have a final TS/SCI clearance without waivers. CSSOs will have the skills, training, and experience to fulfill the specified duties. The senior corporate officer responsible for the SCI Security Program at the contracting corporation will endorse CSSO nominations. Contractors can only serve as a CSSO under a valid contract and must always coordinate their actions through that contract's contracting officer representative (COR). The CSSO will execute the same functions as an SSO as described in paragraph 2-7 and other duties and responsibilities as directed by the SIO through the appropriate contracting officer or COR.

2-8. Special security representative

The SSR is commissioned officer, warrant officer, noncommissioned officer (E-5 or above) or DA Civilian (GS-7 or above), appointed by the SIO, in accordance with DODM 5105.21, V-1, Enclosure 2. The SIO can appoint an SSR at a lower grade without a waiver if personnel of the appropriate grade are not available. The SSR must have a final TS/SCI clearance without waivers. The SSR will implement and manage the SCI Security Program, training, and other requirements for a SCIF, under the direction of the SSO.

2-9. Sensitive compartmented information contract monitor

The SCI contract monitor is a Soldier or DA Civilian of any grade, appointed by the SIO, to oversee the execution of the contract by SCI-cleared contractor personnel. The SCI contract monitor must have a fully adjudicated, final TS/SCI clearance without waivers. The SCI contract monitor will—

- a.* Utilize ACCS, or equivalent approved system, to process all SCI actions.
- b.* Ensure DD Form 254, including all SCI addendums, pre-award, contract award and contract termination/closeout documents are coordinated with the contracting officer or COR and entered into ACCS, or equivalent approved system.
- c.* In coordination with the contracting officer or COR review and approve all extensions, modifications (SF 30 (Amendment of Solicitation/Modification of Contract)) and revisions of DD Form 254/SCI addendum for the prime and subcontracts.
- d.* Ensure that the SCI security requirements are reflected on the DD Form 254 and SCI addendum.
- e.* Review and approve in writing, requests from the CSSO for reproduction and/or destruction of SCI material. Coordinate approval with the document originator prior to authorization.
- f.* Within 30 days of completing a contract, provide written disposition instructions to the CSSO, via the INSCOM contractor support element (CSE), of all SCI material furnished to or generated by the contractor.
- g.* Coordinate with the SSO on the approval of DD Form 254/SCI addendums, extensions, modifications, revisions for continuous access of SCI, and the continued security requirements.
- h.* If required, coordinate with industrial security specialist, SCI contract monitor, and the program office to initiate a national interest determination by ODCS, G-2.

2-10. Sensitive compartmented information indoctrinated personnel

SCI indoctrinated personnel will—

- a.* Adhere to the procedures and requirements outlined in this and other applicable regulations.
- b.* Complete initial SCI indoctrination, including signing Form 4414, SCI security orientation, annual refresher training, and attend debriefings in accordance with paragraph 9-4.
- c.* Successfully complete both initial and annual Cybersecurity Awareness Training concerning wireless use including the vulnerabilities, and threats wireless technology poses in a SCIF.
- d.* Report any violation of this and all applicable regulations in accordance with DODM 5105.21, V-3, Enclosure 5.
- e.* Upon separation from employment, transfer in status, or retirement all SCI-indoctrinated personnel (whether Soldier, DA Civilian, or contractor), sign written agreement to report all employment with foreign government entities for 2 years to the ODCS, G-2 starting on the date of separation, and further to report any change in status of employment with foreign government entities, in accordance with AR 600-291.

Chapter 3

Sensitive Compartmented Information Personnel Security

This chapter implements ICD 704; ICPG 704.1 thru 704.5; DODM 5105.21, V-3; and AR 380-67.

3-1. General

An effective personnel security program is an integral part of an effective SCI Security Program. SCI access is provided only as necessary to fulfill mission requirements. All SCI indoctrinated personnel will ensure compliance with personnel security policies and procedures.

3-2. Approval authority

a. The DNI grants SCI access for individuals in non-national intelligence board government organizations outside of the Army.

b. The DOD CAF grants, denies, or revokes SCI access eligibility in accordance with ICD 704 and its associated ICPGs.

c. Access eligibility determinations based on an exception (deviations, waivers, or contingencies) to ICD 704 personnel security standards or investigation standards are subject to review and acceptance by the DCS, G-2 or designee. The DOD CAF will ensure that the appropriate annotations are made in the Joint Personnel Adjudication System (JPAS) or authorized follow-on system for eligibility determinations based on an exception (deviations, waivers, or contingencies).

3-3. Requirements for sensitive compartmented information access

a. Personnel security standards for investigation and adjudication of eligibility for access to SCI are contained in ICD 704. No person will be deemed to have need-to-know solely by virtue of rank, title, or position. When previously established need-to-know no longer exists due to reorganization, reassignment, change in duties or any other reason, the SCI access approval affected by this change in need-to-know will be terminated and the individual will be debriefed.

b. An initial Tier 5 Investigation (T5) (formerly Single Scope Background Investigation), or Tier 5 Reinvestigation (T5R) (formerly Periodic Reinvestigation) conducted within the last 5 years is the basis for granting access approval for SCI.

c. SIOs may grant access to SCI for Servicemembers and Federal civilian employees under their security cognizance after favorable accomplishment of all of the following:

(1) Prescreening interview prior to indoctrination to SCI.

(2) Validation of the individual's need to know.

(3) Favorable determination of the individual's ICD 704 eligibility by the DOD CAF.

(4) Signing of Form 4414 by the individual. (SF 312 (Classified Information Nondisclosure Agreement) for access to collateral information will have already been executed prior to this requirement.)

(5) Completion of an SCI security indoctrination of the individual including instruction concerning proper handling of SCI information.

d. SIOs may grant SCI access to U.S. contractor employees if all of the following conditions are met:

(1) A DD Form 254 certifies that the contract for which the work will be performed requires SCI access.

(2) The need-to-know for SCI access is determined and approved by the SIO where the work will be performed.

(3) The appropriate U.S. Government COR endorses the requirement.

(4) Favorable determination of the individual's ICD 704 eligibility by the DOD CAF.

(5) Signing of a Form 4414 by the individual.

(6) Completion of an SCI security indoctrination of the individual.

e. Per ICPG 704.4, the DCS, G-2 will accept T5R less than 7 years old as the basis for initial or continuing access to SCI and other controlled access programs.

f. Nominees must not have had a break greater than 24 months in military service or Federal civilian employment or in access to classified information under the National Industrial Security Program.

g. If the individual has a current T5 or T5R which has been adjudicated for SCI access, but is not SCI indoctrinated, he or she must undergo a personal screening interview covering the period since the completion of the last investigation to ensure that he or she continues to meet the standards of ICD 704. The SCI screening interview will be conducted by the SSO or designated security official. If adverse information is disclosed, the DOD CAF will be notified immediately in accordance with AR 380-67 policy on credible derogatory information and the appropriate entries made in JPAS, or authorized follow-on system.

h. Contractor companies must have a final and current facility clearance before contractor personnel may have temporary access to SCI. Valid facility clearances are reciprocal and facility reviews will not be repeated for multiple contracts in accordance with DOD 5220.22-M.

i. The JPAS, or authorized follow-on system, is the DOD personnel security system of record and will be used to record SCI eligibility determinations and indoctrination authority. SCI indoctrinations in JPAS not accompanied by an owning SCI security management office will not be valid. SCI security management office ownership indicates continued and valid need-to-know.

(1) Hardcopy messages (visit/permanent certifications and visit authorization letters) are no longer required for visits involving civilian, military, and contractor personnel whose access level and SCI security management office affiliation are accurately reflected in JPAS (or DOD sponsored follow-on system). It is the responsibility of the individual hosting the visitor to contact the SSO or security manager to validate the individual's security clearance and access level and establish the need to know prior to any meetings and/or release of classified information.

(2) When JPAS is unavailable, the intelligence community's security clearance repository (Scattered Castles) is the alternative "read only" system for verifying clearances and SCI accesses.

(3) In critical situations, SSOs may pass access certifications through secure telephonic means, in advance of the electronic message.

3-4. Sensitive compartmented information access management

a. JPAS, or authorized follow-on system is the source of individual and collective personnel security data that enables effective SCI access management. The DCS, G-2 or designees will manage the granting of SCI accesses in a manner that will—

- (1) Record all SCI indoctrinations and debriefings in JPAS or follow-on system.
- (2) Identify the number of accesses granted, denied, revoked, and suspended.
- (3) Identify investigation date, eligibility date, date of last signed Form 4414, SCI accesses, and exceptions (deviations, waivers, or contingencies).

b. SIOs or designees will further ensure contractor SCI accesses are recorded in JPAS and the Army's ACCS, or equivalent approved system.

3-5. Sensitive compartmented information indoctrination

a. Indoctrination is the instruction provided to an individual prior to receiving access to an SCI system or program. The instructions convey the unique nature, unusual sensitivity, and special security safeguards and practices for SCI handling, particularly the necessity to protect sensitive sources and methods. SCI indoctrination includes the signing of a Form 4414, a briefing on the authorized SCI access, and instructions on the individual's responsibilities.

b. As a condition of access to SCI, individuals must sign a Form 4414 that includes a provision for prepublication review and the following statutes; the Financial Services and General Government Appropriations Act of 2011 (PL 112-74) and the Whistleblower Protection Enhancement Act of 2012 (PL 112-199). Form 4414 establishes explicit obligations on both the Government and the individual for the protection of SCI. A signed Form 4414 is binding for life and cannot be revoked or waived. Failure to sign a Form 4414 will result in denial of SCI access.

c. Form 4414 is unclassified for official use only; however, in certain cases, the fact that a particular person signed a Form 4414 and that the position requires SCI access establishes a relationship that may be classified. The responsible SSO will ensure that a completed Form 4414 is classified, if required by a program classification guide and record it in the appropriate secure system of record.

d. The SSO will determine if an individual has previously signed a Form 4414 by verifying in JPAS, or authorized follow-on system. If verified, no further action is required. If the SSO cannot determine that an individual has signed a Form 4414, the individual will sign a Form 4414 prior to receiving access. There is no prohibition against an individual having more than one signed Form 4414. The SSO will take the following actions in sequence:

(1) Provide the individual with a briefing on the general nature and procedures for protecting the SCI to which he or she will be exposed and explain the purpose of the Form 4414.

(2) Provide the individual the opportunity to read the applicable portions of EO 13526 and statutes cited in the Form 4414. SSOs should respond to Form 4414 related questions should they arise. If questions cannot be answered, the Form 4414 will not be completed until questions are resolved by the appropriate SIO.

(3) Provide the individual an opportunity to express any reservations concerning the execution of the Form 4414 or objection to having SCI access. If an individual declines to sign a Form 4414 as written, he or she will not be indoctrinated or granted SCI access.

(a) The Form 4414 will not be altered by the individual requested to sign it. Because signing the Form 4414 is voluntary, the person administering the Form 4414 must not apply any duress.

(b) Supporting SSOs will coordinate with appropriate offices to ensure that personnel are aware that a position may require the completion of the Form 4414.

(c) The SIO must be advised as soon as possible if an individual refuses to sign a Form 4414.

(4) Instruct the individual to complete the form in ink using his or her signature. The Form 4414 must be completed legibly (printed or typed).

(5) Instruct the witness to sign the Form 4414 in ink. Signing the Form 4414 will be witnessed and accepted for the Government by a military member or a Federal employee. A contractor may not witness or accept the Form 4414.

(6) Annotate JPAS, or authorized follow-on system with the date that the Form 4414 was signed. Organizations administering the Form 4414 may keep a copy if desired and may provide a copy to the individual at the time of completion. If there is no verbal attestation date reflected in JPAS or authorized follow-on system, have the individual read, sign, and date the attestation statement, populate JPAS, or authorized follow-on system with that date, and retain in the attesting individual's personnel security file and uploaded into JPAS.

(7) Indoctrinating SCI official will forward the original, signed Form 4414 to the Chief, Investigative Records Repository (IAMG-C-IRR), 4552 Pike Road, Fort Meade, MD 20755-5995 for archiving.

e. Indoctrination for access.

(1) After the Form 4414 has been signed and accepted, the individual will be fully indoctrinated on the aspects of the SCI compartment to which he or she is eligible and authorized access.

(a) In extreme, mission critical situations an individual (government or contractor) may be indoctrinated for access to SI/TK/G based on an interim or final ICD 704 eligibility determination granted by the DOD CAF. This requirement can only be waived by the DCS, G-2 unless delegated down to ACOMs, ASCCs, DRUs, and ARNG SIOs.

(b) Indoctrination for access to HUMINT Control System (HCS) requires a final ICD 704 eligibility determination granted by the DOD CAF. This requirement can only be waived by the DCS, G-2. The request for waiver will be validated by the SIO and submitted through SSO Army and include the individual's name, rank or civilian grade, Social Security number, date of birth, duty position and justification (classify appropriately and explain why this duty cannot be completed by another properly indoctrinated individual).

(2) SSOs and CSSOs will use the briefing video approved by DIA's Office of Security (SEC), distributed through the SSO Army, as the core indoctrination for access to SI/TK compartments.

(3) SCI indoctrination will describe the specific aspects of the control system requiring protection and advise the recipient of proper channels for reporting matters of security significance, requesting security advice, and determining whether others are authorized access to the control system for which the recipient is approved.

(4) A local SCI security orientation briefing will also be presented and address local security conditions and the command's SCI policy.

(5) SSOs will instruct the individual about republication review requirements prior to public release and about outside activities that could constitute a conflict of interest.

(6) The servicing SSO will immediately update JPAS, or authorized follow-on system to reflect the authorized SCI access for the indoctrinated individual.

3-6. Special circumstances

Refer to the DODM 5105.21, V-3, Enclosure 2.

a. The DCS, G-2 or designee may determine that it is in the national interest to authorize temporary access to SCI before completion of the required investigation.

b. Reservists who will require SCI access for their limited duty tours, but whose weekend duties do not require SCI access, should be provided a special purpose access for the limited tour. SCI access authorized to reservists in connection with their Reserve duties may not be used in connection with civilian or contractor employment.

c. Consultants are authorized SCI access to information specifically identified in the statement of work or consultant agreement.

3-7. Suspension, debriefing, or revocation of sensitive compartmented information access

When the need to know for SCI has ceased or an individual's access to SCI is suspended or revoked, the individual will be denied further access to SCI. The SSO (or CSSO, if appropriate) is responsible for accomplishing and reporting the debrief action in JPAS, or authorized follow-on system, and for canceling all visitor certifications pertaining to the debriefed individual.

a. Individuals who have had their access suspended, or have received a denial or revocation of security clearance, may not enter a SCIF except with SIO approval.

b. At a minimum, debriefings will include—

(1) Reading Section 1 through Section 16, Title 18, United States Code, Appendix (18 USC 1 through 16, Appendix) hereafter referred to as the "Classified Information Procedures Act" or "CIPA" and 50 USC 783, reminding the individual of the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure.

(2) Reading a statement emphasizing the requirement for continued protection of SCI and the responsibilities incurred by the Form 4414. Acknowledgment of the continuing obligation of the individual under the prepublication and other provisions of the Form 4414 never to divulge, publish, or reveal by writing, spoken word, conduct or otherwise, to any unauthorized persons any SCI without the written consent of appropriate department or agency officials.

(3) Reading an acknowledgment that the individual will report without delay to the Federal Bureau of Investigation, or DA counterintelligence personnel, any attempt by an unauthorized person to solicit national security information.

(4) Reminding the individual of the risks associated with foreign travel reporting requirements as applicable.

(5) Signing the debriefing portion of the Form 4414.

(6) Updating JPAS, or authorized follow-on system with the debrief status by the SSO.

c. Upon separation from employment, transfer in status, or retirement as SCI-indoctrinated personnel (whether Soldier, DA Civilian, or contractor), will sign and forward written agreement to report all employment with foreign government entities for 2 years starting on the date of separation and further report any change in status of employment with foreign government entities, in accordance with AR 600–291.

d. SSOs should maintain effective liaison with supervisory personnel to identify as early as possible potential security problems involving SCI-indoctrinated personnel.

(1) When information of a potential security concern develops:

(a) The appropriate commander or SIO will immediately determine if it is in the interest of national security to retain a person in-status, or to take interim action to locally suspend access to SCI pending final resolution of the issue.

(b) The SSO or security manager will expeditiously remove SCI access from JPAS, or authorized follow-on system, and work with the commander or SIO to determine how the issue may affect the individual's continued eligibility for SCI under the ICPG 704.2 and whether the issue requires action by the DOD CAF.

(2) Local SCI access suspension is a temporary measure, including a debriefing, designed to safeguard sensitive classified information or facilities while the issue of concern is investigated. If the incident constitutes credible derogatory information as defined in the AR 380–67, it must be reported to the DOD CAF. The SSO or security manager will submit an incident report via JPAS, or authorized follow-on system. The security manager will submit the JPAS report if collateral access is also suspended.

(a) The JPAS incident report will include the date of the decision as the formal suspension date. The commander, SIO, SSO, or adjudicative authority must notify the individual, in writing, of the formal suspension of SCI access and of the reason for such action.

(b) Follow-up reporting will continue until the individual's commander or SIO has made a final recommendation to the DOD CAF.

(c) Once submitted, only the DOD CAF can make a final determination regarding the individual's continued SCI eligibility.

e. When an individual is debriefed from SCI access because of credible derogatory information, the SSO will submit an incident report via JPAS, or authorized system, to the DOD CAF. The report will specify reason for report, accesses held, indoctrination and debriefing dates, a justification for the debriefing, and any other pertinent information. Individuals debriefed for cause will only be re-indoctrinated following favorable adjudication by the DOD CAF.

f. All personnel who are the subject of an adverse SCI eligibility determination are afforded the opportunity to appeal the determination subject to the provisions of ICPG 704.3. The determination authority is responsible for providing appeal procedures. Reinstatement of SCI access may be granted provided that there is a revalidation of need to know by the responsible SIO or receipt of new favorable SCI eligibility determination by the DOD CAF.

3–8. Reciprocity of accesses (transfer-in-status) individuals

In accordance with ICD 709 and ICPG 704.4—

a. Government civilians and military personnel who temporarily or permanently transfer to another agency may have their SCI indoctrination accesses and supporting documentation passed from the losing organization to the gaining organization only if the gaining organization requires the individual to maintain access to SCI. The transfer eliminates duplication of additional indoctrination paperwork at the gaining organization. A transfer-in-status may be initiated by either the losing or gaining organization's SSO. SSOs will work together to ensure the transfer-in-status is successful prior to the individual leaving the losing organization.

b. Contractor personnel assigned to an Army SCI contract managed by CSE may have their accesses transferred-in-status upon approval from the CSE through the SCI contract monitor. The accesses will be identified on the gaining company's DD Form 254/SCI addendum, the CSE will ensure ICD 704 eligibility requirements are met, accesses are transferred to the company, and annotated appropriately in JPAS and ACCS, or equivalent approved system.

c. In both situations above, it is the responsibility of the losing organization or activity to transmit copies of supporting documentation on individuals transferred.

3–9. Tier 5 Reinvestigation procedures

T5R procedures will be conducted as prescribed in AR 380–67 and in ICPG 704.1.

a. The T5R must be initiated no later than 5 years after the completion date of the last investigation. The individuals concerned will be contacted by their local SCI security official to complete an Electronic Questionnaires for Investigations Processing (e-QIP), to cover the period since the last investigation was completed.

b. The local SCI security official will review completed statements of personal history to determine if they are complete prior to submission to the investigation provider. If the individual fails to submit the requested T5R package, SCI security officials should determine the cause (for example, notification of expiration not received, access no longer required) prior to any automatic termination of SCI access.

3–10. Change in personal status

Individuals with SCI access will notify their respective security office of any significant change in personal status. Failure to comply with reporting requirement may adversely affect an individual's continuing eligibility for SCI access. Significant changes include, but are not limited to, the following:

a. Changes in marital status include marriage, intent to marry, or marriage to a foreign national, divorce, or proposed name change. Cohabitants are treated as spouses in this context. Request for waivers of ICPG 704.4 standards will be reviewed by the DOD CAF on a case-by-case basis. Marriage to, or cohabitation with, a foreign national will be grounds for re-evaluation of SCI access. SCI-indoctrinated personnel will report to the supporting SCI security official or SSO in advance their intention to marry or live with a foreign national. The notification of intent to marry or cohabit will include—

- (1) Complete information of the prospective spouse/cohabitant and his or her immediate family members.
- (2) The type of visa or alien status of the intended spouse or cohabitant and their immediate family members (if resident in the United States, its territories, or possessions), and whether these persons intend to become American citizens.
- (3) The nature and extent of relationship with the intended spouse or cohabitant's family.
- (4) The vocational or political ties of the intended spouse or cohabitant and their immediate family with their government.

b. Change in association with foreign nationals. Contact that is unplanned, non-recurring, with no deliberate effort by either party to affect recurrence is considered casual contact and normally does not require reporting. When casual contact with foreign nationals develops into close and continuous personal associations, or suspicious behavior is noted such as an unusual interest in your employment, the contact must be reported.

c. Other significant changes include, but are not limited to, a legal name change, credit judgments, tax liens, wage garnishments, foreclosures, excessive debt, bankruptcy filing or repossessions, and adverse involvement with law enforcement agencies including arrests for alcohol-related driving infractions. It also excludes traffic offenses when fines are less than \$300 and do not involve alcohol or drugs.

3–11. Employee outside activities

a. Potential conflicts with an individual's responsibility to protect SCI material may arise from outside employment or other outside activity to include contact or association with foreign nationals.

b. Involvement in non-U.S. government employment or activities that raise potential conflicts with an individual's responsibility to protect SCI information is of security concern and must be reviewed by an SCI security official to determine whether the conflict is of such a nature that the individual's SCI access should be reevaluated.

c. Individuals who have or are being considered for SCI access must notify the local SSO of any existing or contemplated outside employment or activity that meets the two criteria below. In addition, an initial or updated copy of the individual's e-QIP must include details of such outside employment or activities.

(1) The term employment or other activity includes compensated or volunteer service with any foreign nation; with a representative of any foreign interest; or with any foreign, domestic, or international organization, or person engaged in analysis, discussion, or publication of material on intelligence, defense, or foreign affairs.

(2) If the employment or activity raises doubt as to an individual's willingness or ability to safeguard SCI information, the servicing SSO will advise the individual that engaging in or continuing such employment or activity may result in withdrawal of SCI access and will provide the individual an opportunity to discontinue such employment or activity. If the individual terminates the employment or activity of security concern, the individual's SCI access approval(s) may be continued provided this is otherwise consistent with national security requirements.

d. The provisions of this section will be made available to individuals to read SCI indoctrination. Annual security education for SCI-indoctrinated individuals will advise them—

- (1) To report in writing to their local SSO any existing or contemplated outside employment or activity.
- (2) That the written report must be submitted before accepting the outside employment or activity.

e. Upon separation from employment, transfer in status, or retirement as SCI-indoctrinated personnel (whether Soldier, DA Civilian, or contractor), will sign and forward written agreement to report all employment with foreign government entities for two years starting on the date of separation and further report any change in status of employment with foreign government entities, in accordance with AR 600–291.

f. In cases where outside employment or association has resulted in a suspected or established compromise of SCI, the local SCI security official and supporting counterintelligence activity must be advised immediately.

3–12. Personnel security files

SSOs will maintain the following information:

a. Personnel security files on each SCI-indoctrinated person during assignment and for a minimum of 180 days after accountability of the person ceases. The files maintained under this provision will include—

(1) Pre-indoctrination screening interview results, Form 4414 (CSSOs will maintain copies of this information in accordance with DD 254 and applicable contract requirements), copies of other pertinent security personnel actions or defensive security briefings and debrief memoranda such as conflict of interest briefings for reservists.

(2) SSOs will send the Form 4414 to the Chief, Investigative Records Repository (IAMG–C–IRR), 4552 Pike Road, Fort Meade, MD 20755–5995 for archiving. The Investigative Records Repository is responsible for retaining in a retrievable manner the original Form 4414 for at least 70 years or until death of the individual. This includes contractor Forms 4414.

(3) Copies of reports of derogatory information, reports of changes in personal status, and other related paperwork such as security violation reports that may adversely affect a person’s continuing eligibility for SCI access or result in referrals to counterintelligence agencies.

(4) Foreign contact reports, foreign travel notifications, foreign travel reports, and the annual briefing on reporting foreign contacts.

b. Justifications for SCI access and approvals or disapprovals will be maintained for 2 years after accountability of the person ceases. (This requirement does not apply to contractors.)

3–13. Security prepublication review process

a. Prepublication review. All proposed public statements on information derived from SCI or concerning SCI operations, sources, or methods must be reviewed and approved before release by the DCS, G–2 or designee. The SSO will establish local written procedures for conducting SCI security reviews or pre-publication reviews. The requirements for SCI security review and prepublication review will be part of the Annual Security Education Program.

(1) The SSO will ensure coordination with the appropriate local government agency public affairs office and legal counsel as part of the review process.

(2) SCI-indoctrinated or debriefed individuals will submit for security review, prior to public disclosure in any form, all material intended for disclosure that may contain SCI or SCI-derived information. The material will be submitted to the organization that last authorized the individual’s access to such information.

(3) The SCI prepublication review does not substitute for or replace any additional prepublication requirements of DODD 5230.09 or other regulations requiring certain military or DOD persons to submit material for review prior to public release.

(4) The security officer receiving the material proposed for publication will make an initial review and coordinate the review as required. If a determination cannot be made initially as to whether SCI is involved, the material will be forwarded through SCI channels to the ACOM, ASCC, and DRU SIOs to ODCS, G–2 for additional review and guidance.

b. Review of resumes and applications for employment. Resumes or applications for employment which detail technical expertise gained through government employment in classified or sensitive programs must not contain classified information even if the potential employer is known to be a cleared defense contractor. A security review should be requested to resolve questions or concerns regarding possible classified content prior to submission to a potential employer.

(1) An SCI-indoctrinated person may indicate the level of their clearance and access to SCI in resumes or applications when seeking employment.

(2) Digraphs or trigraphs will not be included in a resume or job application.

(3) The individual’s servicing SSO or security manager may provide investigation completion dates and case control numbers.

3–14. Contact with foreign nationals

SCI-indoctrinated personnel must protect themselves against cultivation and possible exploitation by foreign nationals who are or may be working for foreign intelligence services and to whom they might unwittingly provide sensitive or

classified national security information. SIOs will develop implementing guidance for the administration of the following policy, as established in ICD 704, for individuals under their security cognizance.

a. Persons with SCI access have a continuing responsibility to report, within 72 hours, to their local SSO (or immediate supervisor if an SCI security official cannot be contacted within 72 hours) all contacts—

(1) In which illegal or unauthorized access is sought to classified, sensitive, or proprietary information or technology, either within or outside the scope of the employee's official activities. Personnel should be skeptical of requests for information that go beyond the bounds of innocent curiosity or normal business inquiries.

(2) With known or suspected intelligence officers from any country.

(3) With, or invitations from, foreign government officials.

(4) In which any foreign national exhibits behavior in a manner where there are indications of foreign intelligence or international terrorist involvement as specified in AR 381–12.

b. Unless specifically approved by the appropriate DCS, G–2, designee, or SIO, SCI-indoctrinated personnel will not initiate contact with foreign government representatives, accept invitations to attend any official or social foreign function, or extend reciprocal invitations. Personnel whose official duties require them to deal officially and socially with foreign nationals must limit their contact and association to the requirements of their duties.

c. Foreign liaison and foreign disclosure personnel and other SCI indoctrinated personnel whose duties require regular official contact with foreign government representatives and other foreign nationals are exempt from the approval requirements and from reporting of foreign contacts directly associated with their duties. The DCS, G–2, designee, or SIO may exempt other personnel, on a case-by-case basis, whose duties require regular contact with foreign nationals.

d. Foreign liaison and foreign disclosure personnel and other SCI indoctrinated personnel whose duties require regular official contact with foreign government representatives and other foreign nationals are not exempt from the 72-hour reporting requirement whenever an incident occurs.

e. The SSO may require the reporting individual to complete a foreign contact questionnaire (see DODM 5105.21, V–3, Appendix 3) based on the foreign contact report. The SSO will forward a copy to the local supporting counterintelligence activity for action and retain an information copy in the individual's personnel security file. Discussions of any contact reports will be restricted to those with a demonstrated need to know. Under no circumstances will the individuals involved, their supervisor, or the local SSO make any attempt to investigate such matters. Investigations of any contact reports will be the responsibility of the appropriate counterintelligence activity.

f. Failure to report foreign contacts as required above may result in reevaluation of eligibility for continued SCI access. This reporting requirement does not imply that an individual will automatically be subject to administrative action if he or she reports questionable contacts or associations.

g. SSOs will ensure that SCI-indoctrinated personnel are briefed annually on their responsibility to report foreign contacts and maintain a record showing the dates that the individuals were briefed.

h. Upon separation from employment, transfer in status, or retirement as SCI-indoctrinated personnel (whether Soldier, DA Civilian, or contractor), will sign and forward written agreement to report all employment with foreign government entities for 2 years starting on the date of separation and further report any change in status of employment with foreign government entities, in accordance with AR 600–291.

3–15. Foreign travel

a. Personnel with SCI access who plan official or unofficial foreign travel will—

(1) Report anticipated foreign travel through their immediate supervisors and to the SSO and complete the foreign travel questionnaire (see DODM 5105.21, V–3, Appendix 4). Failure to report foreign travel may result in reevaluation of eligibility for continued SCI access.

(2) Obtain a defensive travel security briefing or a risk-of-capture briefing from their supporting SSO prior to travel. Briefings provide situational concepts of threats that can be encountered, regardless of the country of intended travel. Threat situations will include those from foreign intelligence services, terrorist or narcotics groups, or indigenous groups active in promoting insurgency, war, civil disturbance, or other acts of aggression.

(3) Report any unusual incidents, occurring during travel.

b. Defensive travel security and risk-of capture briefings.

(1) Defensive travel briefings alert personnel to the potential for harassment, exploitation, provocation, capture, entrapment, or criminal activity and provide courses of action to mitigate adverse security and personal consequences. The briefings also suggest passive and active measures to avoid becoming targets or inadvertent victims. An example of a defensive security briefing is available in the (DODM 5105.21, V–3, Appendix 5).

(2) A risk-of-capture briefing alerts personnel of techniques used to force or trick them to divulge classified information if captured or detained, and suggests courses of action to avoid or limit such divulgence.

(3) Supervisors and security officials will direct personnel to be knowledgeable of threat conditions, monitor the itinerary from a safety point of view, and follow-up on security-related issues.

Chapter 4

Sensitive Compartmented Information Security

4–1. Individuals

Individuals producing SCI material are responsible for properly complying with established security classification guidance and for properly applying that guidance to the material, including all markings required for its protection, control, and dissemination in accordance with AR 380–5. Each individual is also responsible for ensuring SCI material is properly protected in accordance with ICD 703 and DOD 5105.21, V–1. All personnel who produce, transmit, reproduce, or extract SCI from documents or other materials must properly mark and protect the resulting SCI product. They will protect all hard copies, soft copies, and other related media in the same manner as the final material and will report errors in classification and marking, control, or dissemination problems to the responsible SSO. In addition, they will—

a. Include SCI in documents or products only when necessary to accomplish an essential official purpose and produce as few copies as necessary.

b. In developing SCI material, give primary consideration to the intended use of the information and organize the document, if possible, so that SCI can be disseminated separately on a more limited basis such as in an annex or supplement. Review the document before final production to ensure only the minimum scope and level of information essential to the task is included.

c. Produce SCI in a manner that will promote at all times positive control, safeguarding, and need-to-know access only.

4–2. Contractors

Contractors will ensure SCI information in their custody is used or retained only in furtherance of a lawful and authorized U.S. Government purpose. Contractors are required to return all SCI material to the SCI contract monitor or Government program manager when their contract expires or closes out, unless the U.S. Government has given the contractor permission to retain the classified material in accordance with DOD 5220.22–M, Chapter 5. This requirement must be included in item 13 or 14 of the DD Form 254. The information management system employed by the contractor will be capable of promptly facilitating such retrieval and disposition.

4–3. Courier authorizations and requirements

SCI will be transferred by SCI indoctrinated persons, certified or designated couriers, diplomatic pouch, or Defense Courier Service. The SSO, CSSO, or security manager will establish strict accountability and control for courier cards.

a. Couriers will be specifically designated Regular Component Soldiers, Reserve Component Soldiers on orders for active Federal service, U.S. Government civilian employees, DOD contractor when authorized by DD 254, or consultant when authorized by statement of work order. Couriers will have authorized access to the SCI material they are transporting and must be familiar with all rules and regulations governing couriers and transporting information, including hand-carrying aboard military, U.S. Government chartered, or commercial aircraft.

b. Certified couriers are individuals whose primary responsibility is to courier SCI material worldwide.

c. Designated couriers are individuals whose temporary responsibility is to courier SCI material.

d. SCI material will be properly wrapped, per the AR 380–5, prior to giving the material to a courier. When transporting within a single building (military headquarters or DOD controlled building), SCI material will be placed in a locked brief case or locked pouch made of canvas or other heavy-duty material and must have an integral key-operated lock.

e. Two SCI-indoctrinated personnel couriers will be used as a team when transporting SCI beyond the local travel area as a contingency for emergency situations.

4–4. DD Form 2501

a. SSOs and/or security managers will issue couriers DD Form 2501 (Courier Authorization) or equivalent with the acronym “SCI” displayed prominently on one portion of the card. CSSOs are authorized to issue courier orders upon approval from the user agency SCI contract monitor in accordance with the DD Form 254, or if a consultant, a statement of work. Contractor courier orders may be issued as a letter or designated company card and will be controlled to ensure accountability of the program.

b. Couriers will read the appropriate extracts from the espionage laws and execute a certificate acknowledging receipt of the courier card prior to receiving a courier card. (See DODM 5105.21, V–1, Appendix 2.)

4–5. Marking requirements

DODM 5105.21, V–1, Enclosure 4 sets forth specific SCI information security requirements for standard classification markings, marking documents, restricted declassification values and caveats, letters of transmittal, working materials, specialized media, fax control procedures, cover sheets, SCI accountability, storage, temporary release outside of a SCIF, reproduction, transportation of SCI, SCI wrapping requirements, disposition, and destruction and emergency plans. Other related marking requirements are outlined in ICD 710 and on the Security Marking Program webpage on Joint Worldwide Intelligence Communications System (JWICS).

Chapter 5 Security Incidents

5–1. Security incidents

a. General. All actual or suspected incidents of unauthorized disclosure of SCI material will be immediately investigated. SIOs will establish local procedures to guard against, investigate, report, and rectify security incidents or unauthorized disclosures of classified information or systems. In cases where compromise has been ruled out and there is no effect on national security, a common sense approach to the early resolution of an incident at the lowest appropriate level is encouraged. These actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

b. Security incidents. All SCI-indoctrinated personnel will report any security incident affecting or involving SCI to the SSO or local security manager. Security managers will ensure all security incidents involving SCI information are reported immediately to the SSO. The SSO will coordinate and direct the appropriate actions to be taken to respond to the incident, and report the incident immediately in the Army's automated SCI system(s) of record. Security incidents are categorized as either violations or infractions. Security incidents involving classified information may require a preliminary inquiry, hereafter referred to as an inquiry, a security investigation, or both.

(1) *Violations.* A security violation is a disclosure of classified information to persons not authorized to receive it or a serious failure to comply with the provisions of security regulations which is likely to result in compromise. Security violations require an inquiry and/or investigation.

(a) Violations can result from, but are not limited to, deliberate or accidental exposure of SCI to unauthorized personnel resulting from loss, theft, or capture; recovery by salvage; defection; press leaks or public declarations; release of unauthorized publications; or other unauthorized means.

(b) Loss or exposure of SCI from any cause requires immediate reporting, investigation, and submission of a damage assessment describing the impact on national security.

(2) *Infractions.*

(a) An infraction is a security incident involving failure to comply with the applicable security policies or regulatory requirements which cannot reasonably be expected to, and does not, result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent. While it does not constitute a security violation, if left uncorrected, it could lead to security violations or compromises. Security infractions require immediate corrective action but may not require a formal inquiry and/or investigation. Examples of infractions include, but are not limited to, a courier carrying classified documents stopping at a public establishment to conduct personal business, or placing burn bags adjacent to unclassified trash containers.

(b) SIOs, SSOs, and/or management officials will take prompt corrective action on any reported infraction and document the actions taken and recorded in Army's automated SCI system(s) of record.

5–2. Inquiries and investigations

a. Preliminary report of inquiry. When the SCI security official determines that a security violation has occurred, he or she will immediately report the incident to the SIO, and a report of the violation will be forwarded within 72 hours of discovery to SSO DA/DAMI–CDS with information copies to SSO DIA/SEC–1A. (See sample report format in the DODM 5105.21, V–3, Appendix 1 to Enclosure 5.) SSO Army will report the violation immediately to the DCS, G–2 or designee for review and further dissemination in accordance with ICD 701. The local SIO must appoint an inquiry official. Preliminary inquiries will not be conducted by the SSO or SSO staff member. The SSO will brief the appointed inquiry official concerning the conduct of the official inquiry. The SSO will provide status reports to the local SIO and an information copy to SSO DA/DAMI–CDS and SSO DIA/SEC every 30 days until the final report is submitted. Reports will be classified according to the classification level of their content. The inquiry official will provide a final written report of inquiry to the SIO through the SSO. The SIO will refer the incident for formal investigation when the final report of inquiry finds there is a reasonable likelihood of compromise of SCI.

b. Investigation procedures. Preliminary inquiries that determine a potential for SCI compromise should be referred for formal investigation by the SIO to the appropriate authority. An investigation will follow guidance provided in the DODM 5105.21, V-3. "Notwithstanding the provisions in AR 20-1, paragraph 7-11, investigations pursuant to this chapter that involve a senior official are subject to the notification requirement to DA Inspector General, however, the investigation pursuant to this chapter will continue and take precedence over any inspector general investigation."

c. Compromise determination. The investigator will determine the likelihood of compromise, using facts obtained during the investigation, for each security violation. Those determinations will be characterized as—

- (1) *Compromise Certain.* SCI has irretrievably left SCI control channels; uncontrolled dissemination can be confirmed.
- (2) *Compromise Probable.* SCI has left SCI control channels; uncontrolled dissemination may reasonably be expected to occur, but a specific threat cannot be identified.
- (3) *Compromise Possible.* The possibility of uncontrolled dissemination of SCI cannot be ruled out, but with no specific indication to believe such dissemination will take place.
- (4) *Compromise Improbable.* Cases in which uncontrolled SCI dissemination is unlikely, but cannot be positively ruled out.
- (5) *Compromise None.* It is certain that SCI did not leave SCI control channels and was not exposed to unauthorized personnel.

Note. Categories of compromise are further described in DODM 5105.21, V-3.

d. Final report. Reports of investigation will include sufficient detail to explain the incident. (See sample format in the DODM 5105.21, V-3, Appendix 2 to Enclosure 5.) The report will assess intent, location of incident, risk of compromise, sensitivity of information, and mitigating factors in arriving at a final analysis of the incident. All reports will be forwarded through the SCI chain of command to the cognizant security authority.

5-3. Corrective action

a. The appropriate SCI security official will review the final report, advise cognizant SIO of weaknesses in security programs and recommend corrective action. SIOs are responsible to take appropriate corrective action in all cases of actual security violations and compromises. Administrative sanctions imposed in cases of demonstrated culpability will be recorded in security files of the responsible SCI security official. Remedial sanctions according to the severity of the incidents may be applied by the DCS, G-2 or designee.

b. Security deficiencies identified by investigation that contributed directly to the incident will be corrected if it is within the capability of the SIO and the organization concerned. If not, full details and recommendations on corrective measures will be provided to SSO Army with information copy to SSO DIA/SEC-1A.

5-4. Classification review

a. If SCI has been compromised or subjected to risk of compromise, the original classification authority must be contacted. The original classification authority will issue instructions directing one of the following:

- (1) Continue classification without changing the information.
- (2) Modify the specific information, or parts thereof, to minimize or nullify the effects of the reported compromise and retain the classification.
- (3) Downgrade the information.
- (4) Upgrade the information.
- (5) Declassify the information. Lost or compromised documents should be considered for declassification to the fullest extent compatible with national security.

b. The original classification authority will notify the appropriate SCI security official of the results of the evaluation. If any change is made to the classification of the information, the originator will promptly advise all holders of the information.

c. If the classification review determines the lost or possibly compromised information cannot be declassified, the SIO conducts a damage assessment.

5-5. Damage assessments

a. Notices of compromise or requests for damage assessments will be referred to the SIO. The SIO will review the notice or request and task the appropriate element for a damage assessment, if required. Cases involving legal action will be coordinated with the supporting legal activity.

b. The damage assessment will consider how the loss or compromise of the material could result in damage to U.S. national security interests. (For format, see the DODM 5105.21, V-3, Appendix 3 to Enclosure 5).

5-6. Case file retention

Case files referred to the Department of Justice or DOD for a prosecution determination will be retained for 5 years after the closure of the case. All other case files will be retained for 2 years after completion of final action or when no longer needed, whichever is sooner.

5-7. Inadvertent sensitive compartmented information disclosure agreement

The local SCI security official will exercise his or her best judgment to maintain SCI security by seeking written agreements from non-indoctrinated persons to whom SCI was inadvertently disclosed. If the person signs an inadvertent disclosure agreement and the responsible local SCI security official has reason to believe that the person will maintain secrecy concerning the SCI involved, the report of investigation may conclude that no compromise occurred in accordance with DODM 5105.21, V-3, Enclosure 5. Copies of executed inadvertent disclosure agreements will be retained as part of the report of investigation.

5-8. Damaged Defense Courier Service packages

a. If packages are received in damaged condition from the Defense Courier Service, the receiver will send an electronic message to the originator and include the information below. If compromise appears possible, the receiver will also notify the appropriate security official.

- (1) Package number and organization from which received.
- (2) Specific material involved as well as an inventory of all material contained therein.
- (3) Possible cause and extent of damage. Include opinion concerning adequacy of the packaging.
- (4) State if potential compromise of material occurred.

b. The receiver will notify the Commander, Defense Courier Service, via immediate collateral message, whenever SCI material delivered via Defense Courier Service is lost, damaged, compromised, destroyed, or mishandled. Include a statement giving the SCI classification level of the material. Do not identify the specific material in the report.

5-9. Reporting missing sensitive compartmented information—indoctrinated personnel

All personnel who have current SCI access or past access to SCI who are killed, captured, or missing in action, absent without leave, deserters or defectors, or similar circumstances will be reported to the SIO. The SCI security officials will notify SSO Army telephonically and by priority message to SSO DA//DAMI-CDS. In addition to the individual's name, rank, Social Security number, and organization provide a listing or summary of information that may be compromised. Individuals who are killed in action, except SCI couriers or those participating in unauthorized hazardous activities, need not be reported when it is known that death was instantaneous, and no possible interrogation could have occurred. All measures should be taken to resolve the status of the individual as soon as possible.

5-10. Reporting procedures

Report all security incidents involving SCI to the SSO, CSSO, SCI contract monitor, COR, or local security manager. SSO Army will receive a copy of the initial and final report for all security violations.

a. Incidents in which SCI was compromised as a result of espionage or suspected espionage will be reported immediately by the most secure means to the supporting counterintelligence organization, SIO, and SSO Army. Activity concerning the violation will cease pending instructions from the supporting counterintelligence organization.

b. For all other security violations, follow procedures below.

c. SSOs will advise the parent command SCI security officials of SCI security violations occurring within their security cognizance and involving personnel assigned to that parent command.

d. If a security violation is committed by an activity that does not belong to the organization exercising security cognizance over the area where the violation occurred, procedures are as follows:

- (1) The SSO will notify both organizations of the security violation.
- (2) The organization with security cognizance will take the lead and initiate the inquiry and/or investigation.
- (3) A report of investigation will be forwarded to both organizations.
- (4) The organization whose activity committed the violation will determine what corrective action should be taken. The report of this determination will be forwarded to the other organization involved.

e. Security violations occurring on computer systems, terminals, or equipment which process SCI will be reported as soon as practicable, but no later than 24 hours after discovery of the violation, through command SCI channels to the ODCS, G-2 IA division with information copies to SSO Army (HQDA Chief Information Officer/G-6 Data Spillage and Unauthorized Disclosure Policy) and DIA as directed by DODM 5105.21, V-3 and ICD 503. The ODCS, G-2 IA Division will further disseminate reported violations as required. The SSO and the site information system's security official will

coordinate security incidents involving computers. Examples of serious computer security incidents include, but are not limited to—

- (1) Human error in reviewing media for content and classification, resulting in compromise.
- (2) Incorrect setting of security filters that result in the compromise of intelligence.
- (3) Intrusion attempts, either physical or through hacking.
- (4) Virus attacks.
- (5) Failure of a system or network security feature.

(6) Commanders, supervisors, and their security managers must report SCI security violations or other information that could impact on an individual's continued eligibility for access to SCI to the DOD CAF in accordance with security incidents section of this manual and the DODM 5105.21, V-3.

5-11. Reporting/responding to classified information appearing in the public domain or media

a. SCI indoctrinated personnel will not comment on, confirm, or deny information from open source articles or discussions of an SCI nature. They also will not, while accessing the web on unclassified systems, access or download documents that are known or suspected to contain classified information. This includes downloading and viewing on non-government computers such as personal and publicly accessible computers. The publication of SCI in the public domain does not constitute declassification, de-compartmentalization, or relaxation of SCI security policy. Acknowledging information of an unauthorized nature can add to the damage or lend credibility to the information.

b. SCI indoctrinated personnel will report all potentially classified information discovered in the public domain immediately to their security manager and/or SSO.

c. SCI security officials will report through command SCI security channels to the appropriate SIO, SSO Army, and SSO DIA/SEC-1A the publication of actual or apparent SCI information in the public media. For incidents involving contractor information or programs, CSSOs will report through the COR to the appropriate command information security channels to the DCS, G-2 or designee the following information:

- (1) Type of medium (for example book, newspaper, magazine, television, and internet), date of medium, title or headline, and name of author.
- (2) Classified intelligence disclosure. Provide a brief synopsis of information disclosed by public medium (the published information itself should not be transmitted). Identify the classification source of the material.
- (3) The publicly disclosed item (article, book, broadcast transcript, and so forth.) should not be marked to indicate in any way that it contains SCI. The information contained in the item should not be discussed outside a SCIF.

Chapter 6 Physical Security

6-1. Sensitive compartmented information physical security

- a. The DIA/SEC office is the accrediting official for Army SCIFs.
- b. The policy for the administration of physical security and management of SCIFs is prescribed in DODM 5105.21, V-2, Enclosure 2.
- c. The physical security standards for the construction and protection of SCIFs are prescribed in ICD 705, ICS 705-1, ICS 705-2, and IC Tech Spec-for ICD/ICS 705-V1.3.
- d. Operations security (OPSEC) principles are critical for protecting the operational activities and security of SCIFs. OPSEC principles should be considered and implemented based on the local security environment. The facility's location (complete address) and identity as a SCIF will be protected at a minimum of "FOR OFFICIAL USE ONLY (FOUO)". Drawings and diagrams detailing SCIFs should only be posted on unclassified systems when appropriately titled as a "Controlled Space."

6-2. Concept approval for establishing a permanent sensitive compartmented information facility

a. Prior to the establishment of a SCIF, a concept approval memorandum including the justification for establishment of a SCIF will be prepared by the requesting organization. The concept approval is the first critical element in the establishment of a SCIF. The concept approval certifies that a clear operational requirement exists for the SCIF and there is no existing SCIF to support the requirement.

b. Once an operational need for SCI has been identified by the organization, the organization's commander will submit a concept approval request containing the request for SCI and authorization to construct a SCIF to the SIO at the ACOM, ASCC, DRU, or ARNG level for review and approval. This request will identify the SCI required and certify that the organization is able to support the SCIF (that is, manning and budget) throughout its lifecycle.

c. Upon receipt of a concept approval request for a SCIF, the SIO will validate the need for the SCIF and the requirement for the requested level of SCI. The SIOs are required to grant concept approval to establish a SCIF, to include contractor SCIFs, in advance for the mission the SCIF will support.

d. The cognizant SIO will forward the approved concept approval documentation to DIA with a copy to SSO Army.

e. For contractor facilities the SIO will provide the concept approval and, if applicable, the DD Form 254 to DIA with an information copy to the supporting SSO and INSCOM's contract support element through ACCS or follow-on system.

6-3. Temporary sensitive compartmented information facilities

a. T-SCIFs are used in support of tactical, contingency, and field-training operations for a limited time where physical security construction standards associated with permanent facilities are not possible. They may include hardened structures (buildings and bunkers for example, truck-mounted or towed military shelters, tents, prefabricated modular trailers or buildings, and areas used on aircraft and surface and subsurface vessels).

b. ACOM, ASCC, DRU, and ARNG SIOs may establish and grant temporary accreditation to operate a T-SCIF. T-SCIF approvals will be valid for up to 1 year. Consideration must be given to establishing a permanent SCIF whenever it is known that the T-SCIF will be required for a period greater than one year. Extension beyond the 1-year period must be justified in writing and formally approved by DIA before the 1-year period ends.

c. The SSO will forward a copy of message approving T-SCIFs to SSO Army upon receipt for inclusion in the quarterly report to DIA. Upon determination that a T-SCIF is no longer required, a closeout inspection will be conducted by an SCI security official in accordance with DODM 5105.21, V-2, Enclosure 2.

d. Organizations establishing or operating a T-SCIF within a deployed theater will notify the respective Combatant Command SSO within 48 hours. Such organizations will also provide updates relating to the current location and status of T-SCIF under their control as directed by the Combatant Command SSO.

6-4. Temporary secure working area

a. A TSWA is a designated area that can be secured adequately to temporarily handle, process, or discuss classified information, to include SCI, in the absence of an available SCIF. A TSWA will not be used more than 40 hours per month and no longer than 12 months in the same location. ACOM, ASCC, DRU, and ARNG SIOs may approve TSWAs, and will issue a memorandum stating the requirements for each instance of activation and use for the individual TSWA. The 40-hour rule is based on an average use of the TSWA over a 12-month period. TSWA's physical security standards are less stringent than that of a permanently accredited SCIF. If the facility will be used on a more frequent basis, the user of a facility must comply with ICD 705 standards and pursue permanent accreditation. On a case-by-case basis and with sufficient justification, DIA may approve SCI storage (not to exceed 6 months).

b. The SIO may approve TSWAs for all compartments of SCI. Approval for processing SCI in TSWAs may only be granted by DIA or DCS, G-2, according to their respective information system accreditation authority.

6-5. General

Information concerning waivers, mitigations, SCIF design and planning, SCIF types, construction security, SCIF accreditation, and SCIF operations policy guidance is contained in DODM 5105.21, V-2, Enclosure 2.

6-6. Inspection policy

a. SCIF inspections are used to evaluate the implementation of regulations, the security awareness of employees, and existing internal management controls. These inspections at a minimum will include security administration, information security, personnel security, physical security, technical security, and information assurance. Inspections also ensure a SCIF meets the physical, TEMPEST, and automated information system security requirements.

b. The DIA SCIF Management Branch (DIA/SEC) is the authority for DOD SCIF inspections. SCIF inspections will be performed by DIA/SEC, certified SCIF inspectors, with the approval of DIA/SEC prior to accreditation. DIA/SEC is authorized to inspect any accredited SCIF periodically and direct action to correct any deficiency, including removal of SCI facility accreditation.

c. Periodic re-inspections will be incorporated into the Command Security Oversight Program and implemented based on threat, facility modifications, sensitivity of programs, and past security performance at least every three years or immediately upon notification by the accreditation authority, and may occur at any time without regard to normal duty hours. Other authorized inspectors will be admitted to a SCIF without delay after verification of their security clearance information by an SSO/SSR. Inspectors will submit a written report following each inspection, identifying any deficiencies and corrective action to be taken. The report will be forwarded to the SIO and a copy will be maintained within the inspected SCIF and at the accrediting organization.

d. SAVs are a requirement as part of SCI oversight functions in accordance with DOD 5105.21, V-1. SAVs are not inspections but are teaching and training opportunities that support staff inspections. Staff sections conduct SAVs to assist, teach, and train subordinate staff sections to meet the standards required to operate effectively within a functional area. SAVs can occur at the discretion of the commander, SIO, SSO, or a staff principal at any level, who can request a SAV from the next higher staff echelon. SAVs can assist staff SSOs in preparing for upcoming inspections or train staff sections on new security concepts/policies, technologies, or operating techniques. SAVs do not produce formal reports but instead provide feedback to the command and the staff section concerned. Any recommendations that affect physical security, TEMPEST, or technical security will be validated by DIA prior to corrective action or expenditure of funds. SAVs may consist of a complete program review or specific areas within a program.

e. SSOs and SSRs will conduct self-inspections of their SCIFs annually and will use the self-inspection checklist provided by SSO Army. Self-inspections will ensure compliance with the policies and procedures contained in this regulation and other applicable SCI security policies. Self-inspections will be coordinated with the site information system security manager and will include the areas of SCI security policy and procedures, security administration, information security, personnel security, physical security, technical security (TEMPEST and TSCM), and IA.

f. Results of the self-inspections will be routed through the local command channels to the SIO. An annual summary of self-inspection findings and actions will be consolidated at the ACOM, ASCC DRU, and ARNG level and forwarded to SSO Army for review and further dissemination as required.

g. Only SCI-indoctrinated personnel knowledgeable of SCI policies may perform inspections of physical security, information security, personnel security, TEMPEST, security violations, security education, visitor control procedures, and other requirements outlined in this regulation. Inspections by non-SCI indoctrinated entities are limited to the mission of the SCIF, collateral security matters, anti-terrorism/force protection, counterintelligence, operations security, automated information security, and those non-SCI command issues such as safety, fire marshals, supply accountability, crime prevention, readiness, and so forth. Such entities may also review the facility's most recent self-inspection checklist to ensure that the self-inspection was conducted and make note of any discrepancies. Only DIA can direct corrective action when an item affects the physical or TEMPEST accreditation of the SCIF.

h. Entry-exit inspections are conducted randomly and serve to deter unauthorized removal of classified material and to detect introduction of prohibited items or contraband into SCIFs.

(1) SIO's will ensure that all SCIFs under their cognizance have an approved Entry-Exit Inspection Program that will be applicable to all personnel assigned to or visiting the command's SCIFs. The inspection procedures will be reviewed by the supporting legal counsel prior to implementation.

(2) Inspections will be carried out under this program with sufficient frequency to provide a credible deterrent for the unauthorized removal of classified materials or equipment from the SCIF, or the introduction of prohibited items.

Chapter 7

Portable Electronic Devices and Other Prohibited Items

7-1. Personally owned portable electronic devices, including personal wearable fitness devices

a. Personally owned portable electronic devices (PEDs) without audio recording, photographic, video recording, or wireless transmitting capabilities are authorized in Army SCIFs with SSO approval.

b. These devices will never be connected to DOD information technology resources. This includes for recharging.

c. PEDs that are authorized will be approved by the local SSO in writing prior to being brought into the SCIF.

d. Contact SSO Army to obtain current guidance pertaining to PEDs with Bluetooth technology that do not have audio, video, photographic, or other wireless capabilities (that is, personal wearable fitness devices (PWFDS)).

7-2. Restrictions

Only TS//SCI cleared personnel assigned to the SCIF may be authorized to introduce and use PEDs and PWFDS. Visitors will not be authorized to introduce PEDs into the SCIF.

7-3. Misuse or violation of portable electronic device policy

a. Unauthorized use of PEDs jeopardizes the Army's mission, information technology resources and information and may result in administrative, investigative, or disciplinary action. Violations of this policy will follow guidelines addressed under security incidents as outlined in DODM 5105.21, V-3, Enclosure 5. Unauthorized possession or use of any PED may result in its seizure by SSOs or SSRs for the purpose of conducting a forensic or physical examination.

b. All PEDs are subject to inspection at any time. Inspection may result in examination of a PED content and metadata residing on the device. There is not a reasonable expectation of privacy or confidentiality in the content and metadata resident on all PEDs brought into Army SCIFs.

c. Authorized examination of PEDs may result in data loss, compromise of functions, damage, or destruction of the device. In some cases, the devices may be permanently retained, destroyed, or have their data and operation systems sanitized.

d. In accordance with the PED user agreement, a PED seized as evidence of a crime or security violation may be permanently retained, destroyed, or have its data and operating systems wiped resulting in loss of information.

7-4. Additional prohibited items in a sensitive compartmented information facility

Any items that record, transmit, transfer, duplicate, or store data, including photographic equipment, radios, pagers, and headphones with embedded microphones or “noise cancelling” capabilities are prohibited in SCIFs unless specifically authorized by the SSO in writing. Additionally, all items prohibited in Federal facilities which include any item prohibited by any applicable Federal, State, local, and tribal law and/or ordinance, as well as firearms, dangerous weapons, explosives, or other destructive devices (including their individual parts or components) designed, redesigned, used, intended for use, or readily converted to cause injury, death, or property damage, are also prohibited within SCIFs unless specifically authorized by the SSO in writing. Unauthorized items may be seized and turned over to the SSO for appropriate action.

7-5. Exceptions

a. Items needed for medical or health reasons, such as motorized wheelchairs, hearing aids, heart monitors, pacemakers, and insulin pumps may be authorized only if approved by the SSO. A request will be sent to the SSO to review the technical capabilities of the device to determine threats and mitigations. Health or medical equipment that require connection to any device or system which that records, transmits, transfers, duplicates, or stores data, must first be approved by the network designated approval authority prior to their introduction into any Army SCIF. SSOs will work with information systems security personnel to determine capabilities and security risks before granting approval. Compact disks (CD) or digital video disks (DVD) that are “read-only” and do not have the capability to have data written on them, may only be brought in a SCIF after a scan and approval from the organization’s information system security manager.

b. Emergency and police personnel and their equipment, including devices carried by emergency medical personnel responding to a medical crisis or emergency actions (fire drills, police activity, active shooter, alarm failure, power outages, and so forth) within an Army SCIF will be admitted without regard to their security clearance status but must be escorted to the degree practicable. If appropriate, emergency personnel will be debriefed as soon as possible if there are any indications these individuals have been exposed to classified information or information systems.

c. Mission-specific special equipment and personnel may be authorized within a SCIF or other secure areas by the SSO in accordance DODM 5105.21, V-2, Enclosure 4, AR 380-27, and AR 381-14.

7-6. Waivers

a. Requests for exceptions to the policy in this chapter must be submitted in writing through the SSO to the SIO, who will submit the request to SSO Army for consideration. Waivers involving information systems will also be coordinated with the information systems security manager for the affected system. Waivers may be valid for up to 1 year.

b. Submissions must contain a description of the PED or unauthorized device and vulnerability, a justification for the waiver, mission impact if not approved, recommended security countermeasure to apply, residual risk after mitigation to classified information policies or devices that will be used to mitigate the risk of the exception, and acknowledgment by the commander or SIO of the vulnerability and its potential risk to SCI, and acceptance of the risk. Approvals of waivers and/or exceptions (deviations, waivers, or contingencies) will be on a case-by-case basis, and will be made, in writing, by SSO Army.

Chapter 8

Sensitive Compartmented Information Industrial Security Program

SIOs/SSOs are responsible for SCI security management within their organizations and will remain involved in and cognizant of SCI contracting activity within their organizations.

8-1. Appointment of sensitive compartmented information contract monitors

a. When there is a requirement for an Army SCI contract the SIO must appoint a primary and alternate SCI contract monitor in writing as the government official responsible for the command’s Army SCI contract(s).

b. The contract monitor will prepare the DD Form 254/SCI addendum with assistance from the command's industrial security specialist for each prime contract and program requiring access to SCI information. For contractor employee SCI access requirements see paragraph 3–4. A copy of the security section of the statement of work and the DD Form 254/SCI addendum will be reviewed by the industrial security specialist to assist in certifying the security requirements.

c. The SCI contract monitor, SSO, CSSO, and other Government security representatives involved with the processing and oversight of Army SCI contracts will register for an account in ACCS, or in equivalent approved system.

8–2. Contractor and Government sensitive compartmented information facilities

a. Contractors who perform duties inside a Government-owned or controlled SCIF will follow the security policies and procedures contained in Army Regulations. SIOs/SSOs will coordinate with the CSE for guidance and comply with security policies outlined in Army Regulations, the National Industrial Security Program Operating Manual (NISPOM), DOD manuals, and Office of the Director, DNI directives.

b. Commands with contractor SCIFs have the authority to conduct inspections and SAVs after coordination with CSE.

Chapter 9

Sensitive Compartmented Information Security Education, Training, and Awareness Program

EO 13526 and EO 12829 mandate security education. DOD mandates security training for individuals with access to classified information and security education and training requirements for DOD personnel. DODM 5105.21, V–3 also outlines training requirements for individuals appointed duty as SSOs, SSRs, and those granted SCI access. SSO Army promulgates approved training requirements for SSOs and SSRs.

9–1. Requirements for sensitive compartmented information security officials

a. All personnel officially appointed as an SSO will attend DNI- or DIA-sponsored SSO training within 120 days of being appointed.

b. SSOs will ensure ASSOs and SSRs receive the same or similar initial training. ASSOs should receive training within 120 days of being appointed and SSRs should receive training within 30 days of being appointed.

c. Contractor SSOs will have the requisite skills, training, and experience to fulfill their contractually specified duties in accordance with DODM 5105.21 prior to appointment.

d. After receiving initial training, SSOs will attend approved refresher training every 4 years thereafter. SSOs will ensure ASSOs and SSRs receive similar refresher training at 4 year intervals.

e. If approved training as promulgated by SSO Army, is not available, contact SSO Army for further guidance.

9–2. Sensitive Compartmented Information indoctrination and initial security orientation

All personnel will be indoctrinated prior to receiving access to an SCI system or program in accordance with paragraph 3–7. In addition to indoctrination training, individuals being granted access to SCI will receive an initial orientation that covers the following areas in accordance with DODM 5105.21, V–3, Enclosure 6: 1. Threat Awareness and Defensive Security Briefing; 2. Overview of the Security Classification Management System; 3. Explanation of Individual Duties and Responsibilities; 4. Reporting Obligations and Requirements; 5. Submission for Periodic Reinvestigation; 6. Prepublication Review Requirement; 7. IS Security; 8. Marking, Handling, and Safeguarding of Classified Material; 9. Identification of Security POCs; 10. Local Procedures; and 11. Derivative Classification Training.

a. SSOs will also provide security training to subordinate commands for T–SCIF operations and safeguarding of classified information during the pre-deployment phase. In the event the unit has already deployed, coordination will be made with the Combatant Command SSO in the deployed theater to ensure T–SCIF operations comply with all SCI protection requirements.

b. The SCI orientation training above does not replace the requirement for the standardized initial security orientation for all personnel with access to collateral classified information.

9–3. Sensitive Compartmented Information Security Awareness Program

SIOs are responsible to develop and ensure implementation of a continuous SCI security education program that provides security awareness to all SCI indoctrinated personnel. SCI indoctrinated personnel will be advised initially of their responsibility to self-report any activities or conduct that could negatively affect their ability to protect classified information. This training will be documented in writing. The DODM 5105.21, V–3, Enclosure 6 outlines the policy and procedures for developing an effective security awareness program.

9–4. Continuing security annual refresher training and education and awareness

All persons granted SCI access will be trained annually concerning their continuing security responsibilities and security threats they may encounter. All commanders will establish and provide a continuing security awareness program for all SCI indoctrinated individuals under their cognizance. Training provided will keep employees informed of appropriate changes in security regulations, policies, and local requirements, and reinforce the training provided during security indoctrination. Security officials will document in writing the date of the training, subjects covered, the instructor and method of identifying attendees. Records of training will be retained on file for at least 1 year from the date of training. SSOs will provide annual refresher training to, and maintain oversight of SSRs and security managers at all echelons to ensure the integrity of the SCI program.

Chapter 10 General Administration

10–1. Standard operating procedures

SCI security officials will ensure a written SOP is established for SCIFs under their cognizance. SOPs will include site-unique operating procedures and must be reviewed and approved by the SIO annually. The SOP will also be reviewed by the command SSO (ACOM, ASCC, or DRU) and approved by the SIO at the battalion or higher level. These approvals will be documented in writing. SSOs will ensure SOPs are included in the security orientation for newly assigned personnel to the SCIF.

10–2. Defense Intelligence Agency Compartmented Address Book

The DIA Compartmented Address Book (CAB) is a database registry of SSOs or their equivalents in intelligence community organizations. The CAB is a component of DIA's Joint Dissemination System, a web-enabled system accessible via the Joint Worldwide Intelligence Communications System (JWICS), and Secure Internet Protocol Router Network, that allows each SSO to view, add, modify, or delete CAB data as required.

a. The CAB record contains the name of the organization, its major command, SCIFs collateral mailing address, Defense Courier Division address, its Defense Special Security Communication System, and collateral plain language addresses message addresses, contact information for the SCIFs primary and alternate SSO, and the security classification and compartments the SCIF is authorized to receive and maintain. The CAB record also contains an area for the SSO to list all elements they support and free text areas for special instructions and recording JPAS designations.

b. SSOs will access the CAB via JWICS on DIA's Joint Dissemination System and will update the CAB as changes occur.

10–3. Army's Automated Sensitive Compartmented Information Security Program Management System

a. Automated tools issued by HQDA that allow SSOs, SSRs, and SCI security officials to operate, manage, administer, and provide oversight to the Army's SCI Security Program will be utilized upon distribution.

b. All Army military, civilian, and contractor SCI security officials at all levels must utilize distributed systems, and use of all available modules of any system currently in use is mandatory.

Chapter 11 Visitor Control

11–1. Visitor control

The SSO/CSSO/SSR are the authorized officials and points of contact for verification of SCI accesses. The approved DOD clearance verification system for verification of clearances and accesses is JPAS or the Intelligence Community Security Clearance Repository (Scattered Castles), or their authorized follow-on systems.

a. The host facility will limit the access of visitors to areas and SCI required by need to know for official business. The host of a classified conference, meeting, discussion, or video teleconference is responsible for verifying the identity, clearance, accesses, and need-to-know of each person prior to disclosure of any classified information. The host will advise all attendees of the classification level, access level, and dissemination controls or restrictions for the meeting. Access verification procedures will be established by the local SCI security official.

b. Individuals visiting a facility in which there is no capability to verify clearances using JPAS, Scattered Castles, or authorized follow-on system are responsible for requesting their SSO/CSSO/SSR certify their security clearances and accesses to the host facility well in advance of the meeting. Visitors who have not been certified or are not reflected within

JPAS or Scattered Castles of their authorized follow-on systems, will not be allowed access to SCI or permitted to enter SCI facilities until certification is obtained, regardless of the affiliation, rank, or position of the visitor.

11–2. Foreign national visits or sensitive compartmented information facility access

In addition to the requirements outlined in DODD 5230.20 and DODD 5530.3, visitor access to U.S.-controlled SCIFs by foreign nationals will be approved by the SIO based on operational need. Foreign national access to U.S.-controlled SCIFs for an open house, tour, orientation visit, or similar activity is prohibited unless specifically approved by the DCS, G–2 or SIO. The SIO will notify SSO Army as soon as a projected visit by foreign nationals has been confirmed. Requirements for allowing foreign national SCIF access is outlined in DODM 5105.21, V–2, Enclosure 2.

a. Certification. The appropriate security official will certify to the servicing SSO the SCI accesses of foreign nationals authorized to visit Army SCIFs. Certifications received from other than the appropriate security officials are invalid and will not be accepted.

b. Sensitive compartmented information facility access. SCIF personnel will sanitize the SCIF and maintain a low profile to preclude expectations or requests for access.

Chapter 12

Sensitive Compartmented Information Facility Access for the Executive, Legislative, and Judicial Branches

SCI access for the non-DOD executive, legislative, and judicial branches are outlined in DODM 5105.21, V–3, Enclosure 4.

12–1. Executive branch access

The President, Vice President, and Cabinet officers will have access to SCI materials and the DCS, G–2 may grant access without a clearance verification message; the DNI will ensure appropriate security indoctrination. The DNI may grant access to other executive branch personnel when SCI access is necessary for the performance of their duties, following an appropriate security indoctrination briefing in accordance with DODM 5105.21, V–3, Enclosure 4.

12–2. Legislative branch access

a. All legislative branch access to SCI will be conducted in accordance with DODM 5105.21, V–3, Enclosure 4.

b. New SCI information generated through Army programs will be reviewed by the program manager and SSO Army to ensure proper security markings prior to the release to Congress.

12–3. Judicial branch access

All judicial branch access to SCI will be conducted in accordance with DODM 5105.21, V–3, Enclosure 4.

Appendix A

References

Section I

Required Publications

AR 380–5

Department of the Army Information Security Program (Cited in para 2–6*k*.)

AR 380–27

Control of Compromising Emanations (Cited in para 7–5*c*.)
(Available only from Army Knowledge Online)

AR 380–49

Industrial Security Program (Cited in para 1–1.)

AR 380–67

Personnel Security Program (Cited in para 2–4*g*.)

AR 380–381

Special Access Programs (SAPs) and Sensitive Activities (Cited in para 1–1.)

AR 381–14

Technical Surveillance Countermeasures (Cited in para 7–5*c*.)
(Available only from Army Knowledge On-Line.)

AR 600–291

Foreign Government Employment (Cited in para 2–6*g*.)

DOD 5220.22–M

National Industrial Security Program Operating Manual (NISPOM) (Cited in para 1–1.) (Available at <http://www.esd.whs.mil/dd/>.)

DOD 5220.22–M–Sup 1

National Industrial Security Program Operating Manual Supplement (NISPOMSUP) (Cited in para 1–1.) (Available at <http://www.esd.whs.mil/dd/>.)

DODM 5105.21, V–1

Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security (Cited in title page.) (Available at <http://www.esd.whs.mil/dd/>.)

DODM 5105.21, V–2

Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security (Cited in title page.) (Available at <http://www.esd.whs.mil/dd/>.)

DODM 5105.21, V–3

Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special (Cited in title page.) (Available at <http://www.esd.whs.mil/dd/>.)

ICD 701

Security Policy Directive for Unauthorized Disclosures of Classified Information (Cited in para 5–2*a*.)
(Available on JWICS at.)

ICD 703

Protection of Classified National Intelligence, Including Sensitive Compartmented Information (Cited in para 4–1 (intro para).) (Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>).

ICD 704

Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (Cited in chap 3 (intro para).)
(Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>).

ICD 705

Sensitive Compartmented Information Facilities (Cited in para 6–1c.)

(Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>.)

ICD 709

Reciprocity for Intelligence Community Employee Mobility (Cited in para 3–8.)

(Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>.)

ICD 710

Classification and Control Markings (Cited in chap 4-5.)

(Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>.)

ICPG 704.1

Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program (Cited in chap 3 (intro para).)

(Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-policy-guidance>.)

ICPG 704.2

Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (Cited in chap 3 (intro para).)

(Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-policy-guidance>.)

ICPG 704.3

Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes (Cited in chap 3 (intro para).)

(Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-policy-guidance>.)

ICPG 704.4

Reciprocity of Personnel Security Clearance and Access (Cited in chap 3 (intro para).)

(Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-policy-guidance>.)

ICPG 704.5

Intelligence Community Personnel Security Database Scattered Castles (Cited in chap 3 (intro para).) (Available on JWICS at <https://intelshare.intelink.ic.gov/sites/cps/policystrategy/policy/policy%20documents%20series.aspx>.)

ICS 705–1

Physical and Technical Security Standards for Sensitive Compartmented Information Facilities (Cited in para 6–1c.)

(Available on JWICS at <https://intelshare.intelink.ic.gov/sites/cps/policystrategy/policy/policy%20documents%20series.aspx>, under documents click on SCIF Life Cycle Documentation, then click on the ICDs folder.)

ICS 705–2

Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities (Cited in para 6–1c.) (Available on JWICS at <https://intelshare.intelink.ic.gov/sites/cps/policystrategy/policy/policy%20documents%20series.aspx>, under documents click on SCIF Life Cycle Documentation, then click on the ICDs folder.)

IC Tech Spec for ICD/ICS 705, V 1.3

Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (Cited in para 6–1c.) (Available on JWICS at <https://intelshare.intelink.ic.gov/sites/cps/policystrategy/policy/policy%20documents%20series.aspx>, under documents click on SCIF Life Cycle Documentation, then click on the ICDs folder.)

Section II**Related Publications**

A related publication is a source of additional information. The user does not have to read it to understand this regulation. Army Regulations are available on the Army Publishing Directorate website at <http://armypubs.army.mil>. Intelligence

Community directive, policy guidance, standards, and policy manuals are available at <http://www.dni.gov/index.php/intelligence-community/ic-policies-reports>.

AR 1–201

Army Inspection Policy

AR 11–2

Managers' Internal Control Program

AR 15–6

Procedures for Administrative Investigations and Boards of Officers

AR 20–1

Inspector General Activities and Procedures

AR 25–2

Information Assurance

AR 25–30

Army Publishing Program

AR 25–55

The Department of the Army Freedom of Information Act Program

AR 25–400–2

The Army Records Information Management System (ARIMS)

AR 360–1

The Army Public Affairs Program

AR 380–10

Foreign Disclosure and Contact with Foreign Representatives

AR 381–10

United States Army Intelligence Activities

AR 381–12

Threat Awareness and Reporting Program (TARP)

AR 381–20

The Army Counterintelligence Program

AR 381–45

Investigative Records Repository

AR 525–13

Antiterrorism Force Protection: Security of Personnel, Information, and Critical Resources

Army Handbook for Sensitive Compartmented Information Contracts

(Contact DCS, G–2 (DAMI–CDS/Industrial Security Office), 1000 Army Pentagon, Washington, DC 20310–1000.)

DOD 5220.22–R

Industrial Security Regulation (Available at <http://www.esd.whs.mil/dd/>.)

DODD 5230.09

Clearance of DOD Information for Public Release (Available at <http://www.esd.whs.mil/dd/>.)

DODM 5200.01–V1

DOD Information Security Program: Overview, Classification, and Declassification (Available at <http://www.esd.whs.mil/dd/>.)

DODM 5200.01–V2

DOD Information Security Program: Marking of Classified Information (Available at <http://www.esd.whs.mil/dd/>.)

DODM 5200.01–V3

DOD Information Security Program: Protection of Classified Information (Available at <http://www.esd.whs.mil/dd/>.)

DODM 5200.01–V4

DOD Information Security Program: Controlled Unclassified Information (CUI) (Available at <http://www.esd.whs.mil/dd/>.)

DODM 5200.02

Procedures for the DOD Personnel Security Program (PSP) (Available at <http://www.esd.whs.mil/dd/>.)

EO 12333, as amended

United States Intelligence Activities

(Available at <https://www.archives.gov/federal-register/executive-orders/disposition>.)

EO 12829, as amended

National Industrial Security Program (as amended by EO 13691, Sec 6)

(Available at <https://www.archives.gov/isoo/policy-documents>.)

EO 13470

Further Amendments to Executive Order 12333, United States Intelligence Activities (Available at <https://www.archives.gov/federal-register/executive-orders/disposition>.)

EO 13526

Classified National Security Information (Available at <https://www.archives.gov/isoo/policy-documents>.)

ICD 112

Congressional Notification (Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>.)

ICD 501

Discovery and Dissemination or Retrieval of Information within the Intelligence Community (Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>.)

ICD 503

Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation (Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>.)

ICD 700

Protection of National Intelligence (Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>.)

ICD 702

Technical Surveillance Countermeasures (TSCM) (Available at <https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives>.)

ICPG 710.1

Application of Dissemination Controls: Originator Control (Available at <http://www.dni.gov/files/documents/icpg/icpg710.1.pdf>.)

ICS 700–1

Glossary of Security Terms, Definitions, and Acronyms

(Available at <http://www.dni.gov/files/documents/icpg/icpg710.1.pdf>.)

Public Law 112–74

Financial Services and General Government Appropriations Act

Public Law 112–199

Whistleblower Protection Enhancement Act

18 USC Appendix

Classified Information Procedures Act (Sections 1 to 16) (Available at <http://uscode.house.gov/>.)

50 USC 783

Offenses (Available at <http://uscode.house.gov/>.)

50 USC 3003

Definitions (Available at <http://uscode.house.gov/>.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Except where otherwise indicated below, the following DA forms are available on the Army Publishing Directorate website (<https://armypubs.army.mil>).

DA Form 11–2

Internal Control Evaluation Certification

DA Form 2028

Recommended Changes to Publications and Blank Forms

DD Form 254

Department of Defense Contract Security Specification (Available at <http://www.esd.whs.mil/directives/forms/>.)

DD Form 2501

Courier Authorization (Available at <http://www.esd.whs.mil/directives/forms/>.)

Form 4414

Sensitive Compartmented Information Nondisclosure Agreement (Available at <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent>.)

SF 30

Amendment of Solicitation/Modification of Contract (Available at <https://www.gsa.gov/portal/category/21219>.)

SF 312

Classified Information Nondisclosure Agreement (Available at <https://www.gsa.gov/portal/category/21219>.)

Appendix B

Internal Control Evaluation Checklist

B-1. Function

The function covered by this evaluation is the Army SCI Security Program. The following questions are to be used as a template and may vary for your command. These questions should be used as a guide.

B-2. Purpose

The purpose of this evaluation to assist commanders in evaluating the key internal controls outlined below. It is not intended to cover all internal control elements, but focuses upon those that are essential for ensuring effective implementation of the SCI Security Program.

B-3. Instructions

Answers must be based upon the testing of key internal controls such as document analysis, direct observation sampling, simulation, and interviewing. Answers that indicate deficiencies must be explained and the corrective action indicated in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification).

B-4. Test Questions

- a. Has the command established an SCI Security Program?
- b. Has the command appointed in an SIO, SSO, SSR, or CSSO, in writing, to oversee the SCI Security Program?
- c. Are required publications listed in appendix A, section I available to individuals assigned to oversee and manage the SCI Security Program?
- d. Has the command established an SCI self-inspection program for their headquarters and subordinate commands?
- e. Does the command ensure contractors are properly vetted before allowing access to the facility?
- f. Are commands ensuring documentation (SOPs, concept approvals, fixed facility checklist, T-SCIF, TSWA, co-utilizations, memorandum of agreement, and so forth) are reviewed and approved by the SIO/SSO prior to submitting information to DIA or SSO Army?
- g. Are procedures in place to ensure all personnel, including contractors, are aware of the provisions of this publication?
- h. Have SCI security officials (SSOs, ASSOs, CSSOs, and SSRs) received security training?
- i. Are all personnel indoctrinated with access to SCI receiving annual refresher training?
- j. Are incidents and violations reported properly in accordance with this regulation?
- k. Are commands conducting self-inspections and reporting corrective actions on the annual roll-up report to SSO Army?
- l. Are commands completing and providing an accurate annual SCI access report to the DCS, G-2 by reporting the number of personnel indoctrinated in each caveat, indoctrinated in a training position, and indoctrinated with position supporting another ACOM, ASCC, DRU, or field operating agencies?
- m. Have SIOs/SSOs ensured that subordinate SSOs/SSRs are trained, and are in compliance with this regulation, local command policy, and procedures concerning the SCI Security Program?

B-5. Supersession

Not Applicable

B-6. Comments

Help make this a better tool for evaluating internal controls. Submit comment to Headquarters, Department of the Army (DAMI-CDS), 1000 Army Pentagon, Washington, DC 20130-1000.

Glossary

Section I

Abbreviations

ACCS

Army Centralized Contracts and Security Portal

ACOM

Army command

AR

Army Regulation

ARNG

Army National Guard

ASCC

Army service component command

ASSO

assistant special security officer

CAB

compartmented address book

CD

compact disk

CG

commanding general

CIO

Chief Information Officer

COR

contracting officer representative

CSE

contractor support element

CSSO

contractor special security officer

DA

Department of the Army

DCS

Deputy Chief of Staff

DD

Department of Defense forms

DIA

Defense Intelligence Agency

DNI

Director of National Intelligence

DOD

Department of Defense

DOD CAF

Department of Defense Consolidated Adjudication Facility

DODD

Department of Defense directive

DODM
Department of Defense manual

DRU
direct reporting unit

DVD
digital video disks

EO
executive order

e-QIP
Electronic Questionnaires for Investigations Processing

GS
general schedule

HCS
HUMINT Control System

HQDA
Headquarters, Department of the Army

HUMINT
human source intelligence

IC
intelligence community

ICD
Intelligence Community Directive

ICPG
Intelligence Community Policy Guidance

ICS
Intelligence Community Standard

INSCOM
U.S. Army Intelligence and Security Command

JPAS
Joint Personnel Adjudication System

JWICS
Joint Worldwide Intelligence Communication System

NGB
National Guard Bureau

NISPOM
National Industrial Security Program Operating Manual

ODCS
Office of the Deputy Chief of Staff

OPSEC
operations security

PED
portable electronic device

PWFD
personal wearable fitness device

SAP
Special Access Program

SAV

staff assistance visit

SCI

sensitive compartmented information

SCIF

sensitive compartmented information facility

SEC

Office of Security

SECARMY

Secretary of the Army

SIO

senior intelligence officer

SOP

standard operating procedure

SSO

special security office

SSR

special security representative

TEMPEST

telecommunications electronics materiel protected from emanating spurious transmissions

TRADOC

Training and Doctrine Command

TS

top secret

T-SCIF

temporary sensitive compartmented information facility

TSCM

technical surveillance countermeasures

TSWA

temporary secure working area

USD (I)

Under Secretary of Defense for Intelligence

Section II**Terms****Army command**

The highest level of command, designated by the Secretary of the Army (SECARMY), primarily responsible for generating Army forces and planning and executing 10 USC functions.

Army service component command

An operational command, responsible for recommendations to the Joint force commander on the allocation and employment of Army forces within a combatant command. (Source JP 1-02)

Castle Keep

A web-based automation tool that serves as a customer-facing portal to provide business workflow automation services and SCI program reporting, metrics, analysis, and information sharing within the worldwide Army SSO community.

Cognizant security authority

Official with authority over and responsibility for all aspects of management and oversight of the security program established for the protection of intelligence sources and methods, and for implementation of SCI security policy and procedures defined in DNI policies for the activities under their purview.

Command

The authority a commander lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility of effectively using available resources and for planning the employment, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel.

Contractor special security officer

An individual appointed in writing by a cognizant security authority who is responsible for all aspects of SCI security at a U.S. Government contractor facility.

Control system

The top-most level within the Controlled Access Program structure, under which its compartments and sub-compartments reside.

Controlled Access Program

Within the intelligence community, “Controlled Access Program” refers to a top-level control system (such as SI, TK, HCS) and any compartment or sub-compartment under a control system.

Controlled Access Program coordination office

The Director of National Intelligence's focal point for issues dealing with controlled access programs and support to the Controlled Access Program Oversight Committee and the Senior Review Group.

Covered employment

Direct employment by, representation of, or the provision of advice relating to national security to the government of a foreign country for any person whose activities are directly or indirectly supervised, directed, controlled financed, or subsidized, in whole or in major part, by any government of a foreign country.

Direct reporting unit

An Army organization made up of one or more units with institutional or operational support functions, designated by the SECARMY, normally to provide broad general support to the Army in a single, unique discipline not otherwise available elsewhere in the Army. DRUs report directly to a HQDA principal and/or ACOM commander and operate under authorities established by the SECARMY.

Executive branch

The executive branch consists of the President, his or her advisors, and various departments and agencies. This branch is responsible for enforcing the laws of the land. The following are executive branch organizations and agencies: Executive Office of the President (White House), The President's Cabinet (Federal agencies), independent Federal agencies and commissions, USAGov, The Federal Information Center, and FedWorld.

G or GAMMA

Unclassified term used to describe a type of SCI.

Government of a foreign country

Governments of sovereign countries, other than the United States, as well as any person, group, faction, or body of insurgents within a country assuming to exercise governmental authority whether such person, group, faction, or body of insurgents has or has not been recognized by the United States.

Head of the Intelligence Community Element

The head of an agency, office, bureau, or other intelligence element as identified in Section 3 of the National Security Act of 1947, as amended, 50 USC 3003, and Section 3.4(f) (1 through 6) of EO 12333 as amended in EO 13470, Sec. 2. (1.6) and Sec. 4.(d). The DCS, G-2 is the Head of the Intelligence Community Element for the Army.

HUMINT Control System

Unclassified term used to describe a type of SCI.

Indoctrination

Formal instruction to an individual approved for access to sensitive compartmented information or SAPs regarding program-unique information and program-specific security requirements and responsibilities.

Industrial security specialist

The industrial security specialist is the individual designated in writing by the appropriate commander to be responsible for implementing the installation or unit industrial security program, and for providing oversight of contractors who perform classified contractual activities on Army installations or within activities in order to ensure compliance with governing security regulations.

Intelligence community

An element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, by section 3.5(h) of EO 12333.

Internal control evaluation

A periodic, detailed assessment of key internal controls to determine whether they are operating as intended. This assessment must be based on the actual testing of key internal controls and must be supported by documentation (that is, the individuals who conducted the evaluation, the date of the evaluation, the methods used to test the controls, any deficiencies detected, and the corrective action taken).

Judicial branch

It is one of the three branches of government. It consists of the Federal courts (that is, U.S. District Courts, U.S. Courts of Appeals, Territorial Courts), as well as State courts, and is headed by the Supreme Court, which applies the laws to cases that come before it to see if they are Constitutional or not and decides if actions taken by the other two branches (Executive and/or Legislative) are Constitutional or not.

Legislative branch

The legislative branch is made up of the House and Senate, known collectively as the Congress. Among other powers, the legislative branch makes all laws, declares war, regulates interstate and foreign commerce and controls taxing and spending policies. The following are legislative organizations: Architect of the Capitol; Center for Legislative Archives, National Archives and Records Administration; Congressional Budget Office; Government Accountability Office; Government Printing Office; Library of Congress; Office of Compliance; and U.S. Senate.

Local records check

A review of local personnel, post military police, medical records and other security records, as appropriate.

Need-to-Know (or "need-to-know")

The primary security principle in safeguarding SCI is to ensure it is accessible only by those persons with an appropriate clearance, access approval, clearly identified need-to-know, and appropriate indoctrination. Need-to-know exists when a person must have access to classified information to perform a specific and officially authorized function essential to accomplishing a national security task or as required by Federal Statute, executive order, or applicable regulation.

Personal wearable fitness device

Personal wearable fitness device are PEDs that can intelligently measure and store metrics such as the number of steps walked, heart rate, quality of sleep, and other personal metrics.

Personally owned portable electronic devices

Any PED which is not obtained or issued by the Government for use and is not contractor-acquired.

Portable electronic device

PED is any easily transportable electronic device which has a capability to record, copy, store, and/or transmit data, digital images, video, and/or audio. Examples of a PED include, but are not limited to: pagers, laptop computers, cellular telephones, radios (for example, amplitude modulation (AM)/frequency modulation (FM), satellite), compact disc players, cassette players and recorders, personal digital assistants, digital audio, cameras, camcorders, calculators, electronic book readers, personal wearable fitness devices, and electronic watches with input capability and/or reminder recorders.

Refresher training

Refresher training is a refresher of Phase 1 and serve as a constant reminder of an employee's duty, obligation, and responsibility to protect classified information. Refresher training will reinforce the information provided during Phase 1 (security orientation) and will keep cleared employees informed of appropriate changes in security regulations and policies.

Sensitive compartmented information

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

Sensitive compartmented information facility

An area, room, group of rooms, buildings, or installation certified and accredited as meeting Director of National Intelligence security standards for the processing, storage, and/or discussion of SCI.

Single Scope Background Investigation–Periodic Reinvestigation

This investigative product has been replaced by T5R as promulgated in the revised Office of Personnel Management Federal Investigative Standards. A periodic personnel security reinvestigation for TS clearances and/or critical sensitive or special sensitive positions consisting of the elements prescribed in Standard C of ICPG 704.1 initiated at any time following completion of, but not later than 5 years, from the date of the previous investigation or reinvestigation.

Staff assistance visit

A visit by staff members of a particular staff section designed to assist, teach, and train subordinate staff sections on how to meet the standards required to operate effectively within a particular functional area.

Tier 5 Investigation (T5)

Investigation type required for critical-sensitive position and/or TS clearance eligibility special-sensitive position and/or top secret clearance eligibility with SCI. The T5 replaced the Single Scope Background Investigation.

Tier 5 Reinvestigations (T5R)

Investigation type required for critical-sensitive position and/or TS security clearance special-sensitive position and/or Top secret clearance eligibility with SCI periodic reinvestigation. The T5R replaced the Single Scope Background Investigation - Periodic Reinvestigation.

TK

Unclassified term used to describe a type of SCI.

Unauthorized disclosure

A communication or physical transfer of classified information to an unauthorized recipient.

User agency

In accordance with DOD 5220.22–R, this term refers to the Office of the Secretary of Defense (including all boards, councils, staffs, and commands), the DOD agencies, and the Departments of the Army, the Navy, and the Air Force (including all of their activities); the National Aeronautics and Space Administration; the General Services Administration and the Small Business Administration; the National Science Foundation; the Environmental Protection Agency; and the Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor, and Justice; the U.S. Arms Control and Disarmament Agency, the Federal Emergency Management Agency, the Federal Reserve System; the General Accounting Office; and the U.S. Information Agency.

UNCLASSIFIED

PIN 004083-000