Department of Defense

MANUAL

NUMBER 5105.21, Volume 1
October 19, 2012
Incorporating Change 1, Effective May 16, 2018

USD(I)

SUBJECT: Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose, and reissues DoD Manual 5105.21-M-1 (Reference (a)). The purpose of the overall Manual, in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (b)), is to implement policy established in DoD Instruction (DoDI) 5200.01 (Reference(c)), and Director of Central Intelligence Directive (DCID) 6/1 (Reference (d)) for the execution and administration of the DoD Sensitive Compartmented Information (SCI) program. It assigns responsibilities and prescribes procedures for the implementation of Director of Central Intelligence and Director of National Intelligence (DNI) policies for SCI.

b. Volume. This Volume addresses administrative procedures for information security for SCI, including transmission and information systems (IS) security.

2. APPLICABILITY. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoD, the Defense Agencies except as noted in paragraph 2.c., the DoD Field Activities, and all other organizational entities within the DoD (hereafter referred to collectively as the "DoD Components").

b. Applies to contractors in sensitive compartmented information facilities (SCIF) accredited by the Defense Intelligence Agency (DIA) and to DoD SCI contract efforts conducted within facilities accredited by other agencies and approved for joint usage by a co-utilization agreement.

c. Does not apply to the National Security Agency/Central Security Service (NSA/CSS), National Geospatial-Intelligence Agency (NGA), and the National Reconnaissance Office (NRO), to which separate statutory and other Executive Branch authorities for control of SCI apply.

3. DEFINITIONS. See Glossary.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. General procedures for SCI administrative security are found in Enclosure 3 of this Volume. Procedures for information security, transmission security, and information systems security are detailed in Enclosures 4, 5, and 6, respectively, of this Volume.

6. RELEASABILITY. ~~UNLIMITED. This Volume is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.~~ ***Cleared for public release.*** *This volume is available on the Directives Division Website at http://www.esd.whs.mil/DD/.*

7. EFFECTIVE DATE. *This volume is effective October 19, 2012.*

~~a. This Volume is effective October 19, 2012.~~

~~b. If this Volume is not otherwise reissued or cancelled in accordance with DoD Instruction 5025.01 (Reference (e)), it will expire effective October 19, 2022 and be removed from the DoD Issuances Website.~~

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. General Procedures
4. IS
5. Transmission Security
6. IS Security

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD 5105.21-M-1, "Department of Defense Sensitive Compartmented Information Administrative Security Manual," August 1998 (hereby cancelled)
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," ~~November 23, 2005~~ *October 24, 2014, as amended*
(c) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," ~~October 9, 2008, as amended~~ *April 21, 2016*
~~(d) Director of Central Intelligence Directive 6/1, "Security Policy for Sensitive Compartmented Information," March 1, 1995[1]~~
(d) Intelligence Community Directive 703, "Protection of Classified National Intelligence, including Sensitive Compartmented Information," June 21, 2013[1]
~~(e) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012~~
(f) Intelligence Community Directive 701, "Security Policy Directive for Unauthorized Disclosures of Classified Information," March 14, 2007
(g) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011*, as amended*
(h) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
(i) Parts 160 and 164 of Title 45, United States Code
~~(j) DoD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public," July 22, 2005~~
(j) DoD Directive 5210.50, "Management of Serious Security Incidents Involving Classified Information," October 17, 2014
(k) DoD Manual 5200.01, "DoD Information Security Program," Volumes 1-4, February 24, 2012
(l) Executive Order 13526, "Classified National Security Information," December 29, 2009
(m) National Security Agency, "Signals Intelligence Security Regulation (SISR)," May 26, 1999 (Classified SECRET//SI)[2]
(n) National Security Telecommunications and Information System Security Advisory Memorandum (NSTISSAM) 2-95, "RED/BLACK Installation Guidance," December 12, 1995[2]
(o) Intelligence Community Directive 501, "Discovery and Dissemination or Retrieval of Information Within the Intelligence Community," January 21, 2009
~~(p) Director of Central Intelligence Directive 6/7, "Intelligence Disclosure Policy," June 30, 1998[1]~~
(p) Intelligence Community Directive 403 "Foreign Disclosure and Release of Classified National Intelligence" March 13, 2013

~~[1] Available via JWICS at http://www.intelink.ic.gov/sites/ppr/policyHome/default.aspx.~~
[1] Available via JWICS at https://www.intelshare.intelink.ic.gov/sites/odnipolicystrategy/policy/SitePages/Policy%20Home.aspx
[2] Available via JWICS at http://inteldocs.intelink.ic.gov/view.php?kt_path_info=ktcore.actions.document.view&fDocumentID=3508231

(q) "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (short title: "National Disclosure Policy (NDP-1)), October 2, 2000 (Classified SECRET//NOFORN)
(r) Director of Central Intelligence Directive 6/6 (Section V-X), "Security Controls on the Dissemination of Intelligence Information," June 11, 2001
(s) Intelligence Community Directive 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 1, 2008
(t) Intelligence Community Directive 705, "Sensitive Compartmented Information Facilities," May 26, 2010
(u) Defense Intelligence Agency Directive 8500.002, "Department of Defense (DoD) Secure Compartmented Information (SCI) DoD Intelligence Information System (DoDIIS) Community Information Assurance (IA) Program," March 20, 2008[3]
(v) Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008
(w) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006*, as amended*
(x) Intelligence Community Directive 710, "Classification and Control Markings System," September 11, 2009
(y) Controlled Access Program Coordination Office Authorized Classification and Control Office (CAPCO) Markings Register, Volume 4, Edition 1 (version 4.1), December 10, 2010[1]
(z) Section 2014 of Title 42, United States Code
(aa) Section 3302 of Title 44, United States Code
(ab) National Computer Security Center Technical Guidance (NCSC-TG) 025, "Guide to Understanding Data Remanence in Automated Information Systems," October 2002[2]
(ac) Committee on National Security Systems Instruction 4004.1, "Destruction and Emergency Protection for COMSEC and Classified Material," August 2006[3]
(ad) Department of the Interior Acquisition Regulation 35-2, "Circuitry Handling Sensitive Compartmented Information," May 24, 1999[3]
(ae) DoD Instruction 8560.01, "Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing," October 9, 2007
(af) National Security Telecommunications and Information Systems Security Instruction 3030, "Operational Systems Security Doctrine for the FORTEZZA PLUS (KOV-14) and Cryptographic Card and Associated Secure Terminal Equipment (STE)," October 26, 2001[2]
(ag) National Security Telecommunications and Information Systems Security Instruction 3013, "Operational Security Doctrine for the Secure Telephone Unit III (STU-III) Type I Terminal," February 08, 1990[3]
~~(ah) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002, as amended~~
~~(ai) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003~~
~~(aj) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007~~
(ah) DoD Instruction 8500.01, "Cybersecurity," March 13, 2014

[3] Available via SIPRNET at http://www.diateams.dse.dia.smil.mil/sites/issuances/default.aspx.

(ai) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in accordance with Reference (b), serves as the senior DoD official for oversight of implementation of SCI security policies and procedures within the DoD. As such, the USD(I) represents the Secretary of Defense when coordinating SCI security policies and procedures established by the DNI. The USD(I) has established the Defense Special Security System (DSSS) to administer the SCI program within the DoD.

2. DIRECTOR, DIA. The Director, DIA, serves as the Director of a Defense Agency, as the Head of a DoD Component, and as the Head of an Intelligence Community Element (HICE). In accordance with Reference (c), and under the authority, direction, and control of the USD(I), the Director, DIA, shall:

a. Administer the DoD SCI security policies and procedures consistent with DNI policies and procedures to protect intelligence and intelligence sources and methods.

b. Develop and implement standards for and oversee the operations of all SCI compartments for the DoD Components. In this capacity, the Director, DIA, shall:

(1) Direct, manage, and oversee the DSSS.

(2) Appoint a cognizant security authority (CSA) to serve as the authority for all aspects of security program management for the protection of SCI. This individual will also act as the CSA for OSD, the Chairman of the Joint Chiefs of Staff and Joint Staff, the DoD Field Activities, and the Combatant Commands and may delegate CSA responsibilities as necessary.

(3) Review and approve proposals for establishing new SCI security offices under the DIA CSA.

(4) Provide SCI security program direction, management, and oversight to the Military Departments.

(5) Administer SCI security support to other Federal agencies by special agreement as required.

(6) Administer uniform DoD SCI policy on the interrelated disciplines of information security, personnel security, physical security, technical security (e.g. TEMPEST and technical surveillance countermeasures (TSCM)), information assurance (IA), security education and awareness, and contractor SCI program administration to implement and supplement National Intelligence Board (NIB) and DNI SCI policy.

(7) Enforce DoD compliance with DoD and DNI SCI policy, correct deficiencies, and conduct inspections of DoD SCI facilities.

(8) Establish procedures with the Military Department HICEs to coordinate and accomplish program reviews and inspections to eliminate scheduling conflicts.

(9) Provide centralized physical security and TEMPEST accreditation for the DoD Components and DoD contractors except those under the security cognizance of NSA/CSS, NGA, and NRO. This authority may be delegated to a single official, who shall serve as the Accrediting Official.

(10) Validate and maintain records of waivers for DoD SCI facilities.

(11) Establish, manage, and conduct training programs for SCI security officials and other security personnel.

(12) Establish an SCI Policy Coordination Committee (SCIPCCOM).

(13) Develop and publish uniform SCI briefing materials for SCI indoctrination, debriefing, and execution of nondisclosure agreements (NdA) and nondisclosure statements (NdS) for the DoD Components. The indoctrination and debriefing materials shall emphasize awareness of unauthorized disclosure processes and individual reporting responsibilities. On a periodic basis, produce SCI security education materials for the DoD Components.

3. HEADS OF DoD COMPONENTS THAT ARE NOT ELEMENTS OF THE INTELLIGENCE COMMUNITY. The Heads of DoD Components that are not elements of the intelligence community shall appoint, at an appropriate level, a senior intelligence official (SIO) who shall be responsible for the overall management of SCI programs and that portion of the DSSS within their Component. This appointment shall be reported to DIA and the USD(I).

4. HEADS OF THE INTELLIGENCE COMMUNITY ELEMENTS OF THE MILITARY DEPARTMENTS. The HICEs for the Military Departments shall:

a. Administer the SCI security programs for their respective Departments and component commands of the Combatant Commands. Military Department execution will be based upon guidance in this Manual.

b. Provide implementing instructions for the operation and administration of SCI security programs for their respective agencies, departments, and components, including subordinate commands of the Combatant Commands, in accordance with this manual.

c. Assist the Director, DIA, in developing and recommending appropriate SCI security policy and procedures. Appoint a knowledgeable SCI security policy representative to the SCIPCCOM.

d. Appoint a CSA to manage, operate, and administer for their respective Military Departments a special security officer (SSO) system that is part of the DSSS and approve concept proposals for establishing new SCI security missions and facilities under their authority.

e. Conduct a continuing review of their Military Department SCI security programs, including oversight and evaluations. Review and evaluation of SCI security programs shall include site visits and direct contact or visitation with site personnel. Oversight visits shall include oversight of compliance with this Manual. Deficiencies shall be documented and reports of the status of corrections provided to the CSA.

f. Establish, manage, and conduct training programs for Military Department SCI security officials to enable them to perform the duties and meet the requirements contained in the appropriate regulations and directives.

g. Establish procedures to properly investigate security violations, compromises, and unauthorized disclosures of SCI in accordance with Intelligence Community Directive (ICD) 701 (Reference (f)) and to refer results to the supporting counterintelligence agency in accordance with DoDD 5240.06 (Reference (g)).

h. Provide SSO-related resources (e.g. funding and manpower) and resource management guidance to facilities under their authority for the proper administration of SCI security programs within their Departments. Provide for the dedicated funds and manpower needed to manage and operate their special security offices.

i. Establish, manage, and conduct formal continuing security awareness training, and education programs to ensure complete, common, and continuing understanding and application of SCI security under this manual.

5. CSAs. The CSAs shall, as delegated by the HICE, 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 DNI policies for the activities under their purview. CSAs may formally delegate this responsibility to specific elements within their organization

6. DoD COMPONENT SIO. The DoD Component SIO shall:

a. Be responsible for the command's SCI security program. The SIO or his delegated designee shall appoint in writing a Component SSO to directly support the SIO and all primary and alternate SSOs, special security representatives (SSRs), IA managers (IAMs), IA officers (IAOs), and control officers as required for all authorized SCI compartments (e.g., Talent Keyhole, GAMMA, Human Intelligence (HUMINT) control system). Appointments shall be maintained locally. The Component SSO will be functionally subordinate to the SIO and be a member of the SIO staff. The Component SSO shall be responsible for a component's SCIFs,

provide direct support to other SSOs, SSRs, or contractor SSOs and have direct access to the SIO.

b. 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 standard operating procedures (SOPs) and practices.

c. Maintain the integrity of the SCI control system. SSO and contractor special security officer (CSSO) personnel shall not perform duties or details that conflict or interfere with their SCI security responsibilities or with the security of SCI.

d. 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 IS.

e. Identify required communications electronics and communications security (COMSEC) equipment to local supporting communications elements. Establish a memorandum of agreement (MOA) with the supporting communications element to provide timely communications support to the intelligence mission, if necessary.

f. Establish MOAs with other organizations, as necessary, on SCI areas of responsibility, training, operational needs, support, and services. Implement SOPs as required for further definition and clarification of security responsibilities.

g. Establish a co-utilization agreement (CUA) between the SSO and the local program security officer for any special access program (SAP) operating in the SCIF and monitor compliance with the CUA.

h. Train SSOs and SSRs to perform their respective duties and responsibilities.

i. Provide sufficient qualified personnel, funds, work space, facilities, and logistical support to effectively operate the SCI security program.

j. Evaluate and send to the Defense Messaging System requests to use the Defense Special Security Communication System (DSSCS) for SAPs and other special programs or projects.

k. Request that DoD Component counterparts responsible for military police activities direct subordinate military police activities to provide SSOs all derogatory information on SCI-indoctrinated personnel.

l. Keep the SSO informed of issues having SCI implications such as facilities utilization, IS requirements, base security, or base or post resource protection.

m. 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.

n. Coordinate and approve or disapprove requests for waivers as designated in this Manual.

o. Validate the need to establish SSOs or SSRs at locations under their authority.

p. Provide direction to Contracting Officer's Representatives involved in SCI contracts to coordinate DD Form 254, "Contract Security Classification Specification" with the SSO for proper approval. (DD Forms and Standard Forms (SFs) can be obtained on the Internet at http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.)

q. Request that DoD Component counterparts responsible for medical services direct subordinate medical services activities to:

(1) Provide SSOs information about a person's medical condition affecting their continued eligibility for SCI access and information concerning treatment that may temporarily affect an individual's ability to perform SCI duties in accordance with DoD 6025.18-R (Reference (h)).

(2) Facilitate requests for such information from non-DoD sources in accordance with Parts 160 and 164 of title 45, Code of Federal Regulations (Reference (i)).

SSOs must provide such information to the appropriate central adjudication facility (CAF) for a determination of SCI eligibility.

r. Properly investigate security incidents, compromises, and unauthorized disclosure of SCI in accordance with Appendix 1, Enclosure 5, Volume 3 of this Manual; Reference (f); DoDD 5210.50 (Reference (j)) and DoDM 5200.01 (Reference (k)), and refer results to the supporting counterintelligence agency in accordance with Reference (g).

7. COMMANDERS AND CORPORATE OFFICIALS. Commanders and responsible corporate officers whose unit or organization does not have an assigned SIO and operates a SCIF are responsible for the proper management and oversight of that SCIF. These individuals will:

a. Approve all SOPs and Emergency Action Plans (EAPs) pertaining to their SCIFs.

b. Appoint in writing all SCI security officials within their organizations.

c. Oversee the protection of SCI through a comprehensive inspection program that includes self-inspections and random command/corporate-level reviews.

8. SECURITY OFFICIALS. Security officials provide SCI advice and assistance and normally have day-to-day SCI security cognizance over their offices or subordinate SCIFs. Assignment as the SSO or CSSO is a primary duty and they will not be assigned duties or details that conflict or interfere with performance of SCI control responsibilities. Assignment of an SSO in an S-2, G-2, N-2, J-2, or command security office position does not constitute a conflict of interest.

9. SSOs AND CSSOs. SSOs and CSSOs manage the SCI security program and oversee SCI security functions for subordinate SCIFs. Contractors can only serve as a CSSO under a valid contract and must always coordinate their actions through that contract's COR. SSOs will be military commissioned officers, warrant officers, non-commissioned officers (E-7 or above), or civilians (GS-9 or above). 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. This official may nominate himself or herself as a CSSO. All references to SSOs throughout the remainder of this Manual are inclusive of CSSOs unless otherwise noted. SSOs will be indoctrinated for all SCI compartments that their activity is authorized. SSOs shall:

a. Supervise the operation of the special security office and administer the SCI security program to include SCI security oversight for other SCIFs under the organization's security cognizance.

b. Maintain applicable SCI directives, regulations, manuals, and guidelines to adequately discharge SSO duties and responsibilities.

c. Properly account for, control, transmit, transport, package, and safeguard SCI. Provide for destruction of SCI by authorized means and in accordance with this Manual and DD Form 254, as appropriate.

d. Disseminate SCI only to persons authorized access to the material and having an established need to know.

e. Serve as the official channel for certifying and receiving SCI visitor clearances and accesses.

f. Maintain the Joint Personnel Adjudication System (JPAS) to accurately reflect all personnel under their cognizance.

g. Conduct or otherwise manage SCI personnel, information, physical, and technical security (e.g. TEMPEST and TSCM) actions and procedures in accordance with this Manual.

h. Provide guidance and assistance for processing SCI position and eligibility requests.

i. Perform all aspects of the SCI Personnel Security Program to include, but not limited to, nomination interviews, validation of SCI access requirements, submission of investigative requests, conduct SCI security briefings; obtain signed NdA and NdS; and perform other related personnel security actions. (Supporting SSOs will provide this service for contractors unless it is specifically delegated to the CSSO by the owning SSO of the contract.) Provide a briefing on local SCI security procedures to newly-arrived personnel and those receiving initial SCI indoctrination. Emphasize unauthorized disclosure awareness, management, and reporting during indoctrination and termination briefings and day-to-day security program execution.

j. Direct each subordinate SCI official to conduct an annual self assessment and forwards it for SSO review within 14 days of completion. SSOs shall annually report to the DIA Deputy Director for Mission Services, Counterintelligence and Security Office (DAC) the results of the self-inspections along with action taken to address any shortcomings.

k. Report and investigate all unauthorized disclosures of classified intelligence information in accordance with this Manual and References (f), (j) and (k).

l. Interface with telecommunications centers, IS facilities, computer centers, and similar offices to establish and maintain SCI security operational channels. Provide telecommunications centers, watch centers, and the appropriate command centers with the non-duty telephone numbers of, and instructions for, contacting special security office personnel.

m. Conduct a continuing SCI security education training and awareness program to ensure all SCI-indoctrinated individuals are kept apprised of the requirements and guidelines for protecting SCI. Annual training of original classification authorities and biennial training derivative classifiers required by Executive Order 13526 (Reference (l)) will be included in this program.

n. Maintain appropriate accreditation documentation for each SCIF, communications system, and IS under the organization's security cognizance.

o. Review all reported derogatory information on SCI-indoctrinated personnel. Take appropriate action as required by applicable DoD personnel security regulations described in Enclosure 1 of Volume 3 of this Manual.

p. Manage, supervise, and provide support to special access programs (SAPs) based on approved co-utilization agreements.

q. Provide SSO support to DoD SCI contractors in accordance with applicable contracts, including processing, reviewing, and validating DD Form 254. Support provided to contractors of other components will be provided as agreed to in MOAs with user agencies. (This duty does not apply to CSSOs.)

r. Maintain continuing liaison, as required, with non-SCI security officials.

10. SSRs and CONTRACTOR SPECIAL SECURITY REPRESENTATIVES (CSSRs). SSRs and CSSRs, under the direction of their supporting SSOs, are responsible for the day-to-day management and implementation of the facility's SCI security program for subordinate SCIFs. For all SCIFs in which no SSO is resident, an SSR shall be appointed in writing. SSRs and CSSRs perform one or more of the SSO duties listed above as delegated and agreed to by their SSOs. SSRs will be SCI-indoctrinated military commissioned officers, warrant officers, non-commissioned officers (E-5 or above), or civilians (GS-7 or above). CSSRs will have the skills, training, and experience to fulfill the specific duties. The cognizant SIO may appoint SSRs at a lower grade level without further waiver with sufficient justification.

11. COR/ CONTRACTING OFFICER TECHNICAL REPRESENTATIVE (COTR). A COR/COTR who is responsible for overseeing performance of contracts involving SCI information or material shall be SCI-indoctrinated Government personnel who are familiar with the daily operational requirements of contract execution. The COR/COTR shall:

a. Provide DD Form 254 to the supporting organizational SSO for approval prior to incorporation in the contract.

b. In conjunction with the designated contractor representative or CSSO, prepare the initial request for establishment of a contractor SCIF, if required by the DD Form 254.

c. If a Defense Courier Division (DCD) account is required by the SCI contract, prepare a Defense Courier Account Record form and have the supporting SSO sign as the certifying official. Forward the original U.S. Transportation Command Defense Courier Account Record form and a copy of the DD Form 254 (if applicable) to the servicing DCD facility.

12. INDIVIDUALS WITH SCI ACCESS. Each individual who has access to SCI shall:

a. Report to proper authorities (SSO, security official, supervisor) any information that could reflect on their trustworthiness or on that of other individuals who have access to SCI, such as, but not limited to things such as:

(1) Violation of security regulations.

(2) Unexplained affluence, financial delinquency, garnishment of wages, lien placed on property for failure to pay a creditor, bankruptcy, or excessive indebtedness.

(3) Unlawful acts, except for traffic offenses where fines are less than $300 and do not involve alcohol or drugs.

(4) Apparent mental or emotional problems.

(5) Coercion or harassment attempts.

(6) Blackmail attempts.

(7) On-going contacts with foreign nationals.

(8) Planned or actual cohabitation with or marriage to a foreign national.

(9) Foreign travel (official and unofficial).

(10) Arrests, whether or not found guilty.

(11) Alcohol incidents, DUI arrest, obtaining alcohol abuse counseling or treatment.

(12) Use, possession, or acquisition of illegal or illicit substances; misuse of prescription drugs.

b. Immediately report an actual or potential security violation or compromise to an SCI security official (SSO/SSR). In addition, individuals shall report any unauthorized disclosure or exposure of SCI that might reasonably be expected to result in the publication of SCI in the public media such as newspapers, books, television, radio, and internet blogs.

ENCLOSURE 3

GENERAL PROCEDURES

1. GENERAL

a. Users should refer to DCIDs, ICDs, intelligence community (IC) policy memorandums and guidance, DoD issuances, the Signals Intelligence Security Regulation (Reference (m)), National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) 2-95 (Reference (n)), and other documents cited herein for guidance on classification level, compartmentalization, decompartmentalization, sanitization, release to foreign governments, emergency use, and additional security policy and procedures for the protection of information controlled in SCI compartments.

b. Recommendations on SCI policy changes made by the DoD SCI security community shall be raised at the SCIPCCOM. This committee, chaired by the Chief, DIA DAC or designee, is composed of senior SCI security policy representatives of the USD(I) and the Military Departments. This committee shall meet at least semi-annually and the chairperson shall forward recommendations to the security directors of DIA and the Military Departments for presentation to the DNI Special Security Center as appropriate.

c. Information sharing has become a critical component of providing our war fighters the required intelligence information when needed. ICD 501 (Reference (o)) sets forth guidance on sharing intelligence information. The goal of information sharing is to provide appropriately cleared customers (i.e., those with the necessary clearance, access approval, and need to know) with all the intelligence information they need to fulfill their missions.

d. The procedures set forth in this Volume are the standards for protecting SCI. The DoD Components shall not establish or disseminate operational or administrative procedures inconsistent with the security standards prescribed herein. HICE may impose more stringent procedures if they believe extraordinary conditions and circumstances warrant.

e. In emergencies or when there is a danger of compromise, the DoD Components and DoD contractors are authorized to communicate directly with the DAC concerning SCI policy matters. All other matters should be resolved through the established chain of command.

f. During hostilities, wartime, or exercise conditions, the authority and reporting channels for SCI security cognizance shall run parallel to the theater command and operational lines of authority. This procedure exists because staff oversight of SCI security is the direct responsibility of the SIO responsible for the theater. The SSO of the Combatant Command has SCI security cognizance for units deployed in the Combatant Command's theater of operations.

g. Service Cryptologic Components, those Military Service elements that are assigned to the CSS, are under the direction and management of the Director, NSA/Chief, CSS, for physical,

TEMPEST, and IS security matters. Any SCI policy conflict shall be resolved by negotiation between the Military Department and NSA.

2. RISK MANAGEMENT

a. SCI security officials shall employ the principles of risk management and risk-based analysis when developing and implementing protective measures. Risk-based analysis should provide for increased efficiency of operations and co-utilization of facilities wherever practical. SCI security officials shall request waivers to SCI security policy from their respective CSAs and justify the need for deviation from established security methods.

b. SCI security officials shall obtain a threat assessment of the current criminal, espionage, sabotage, subversion, and terrorist threat situation from their supporting law enforcement agency and counterintelligence support office or equivalent. Security countermeasures to meet these threats shall be tailored based on risk management.

3. DIRECT REPORTING/COMMUNICATIONS AUTHORIZED. Each DoD Component shall establish procedures for SCI security officials to communicate directly with the appropriate HICE or designee on emergency matters that affect plans or operations when there is a danger of compromise and the established chain of command cannot be followed. SCI security officials under the cognizance of the SSO DIA security authority may communicate directly with the SSO DAC on emergency matters where SCI is in imminent danger of compromise. At all other times, SCI security officials shall follow their chain of command for the processing of SCI-related matters. Contractors shall go through the contracting officer to the organization that issued the contract.

4. PUBLIC DISCLOSURE OF CLASSIFIED INFORMATION

a. SCI shall not be published, released to, or discussed with, unauthorized persons or the public media. HICEs shall not authorize declassification of SCI for public release without the prior written approval of the appropriate DNI security executive agent. Requests for such declassification action shall be forwarded through command SCI security channels to the appropriate DNI executive agent. Requests for news media information shall be forwarded through the appropriate command SCI security channels to the appropriate HICE or designee.

b. Unauthorized disclosure of SCI (disclosure that has not been approved for release by the HICE or appropriate DNI security executive agent) in public media does not alter the basic security policies and procedures contained in this Manual or the information's original classification. Such information remains classified. Individuals are not relieved of their obligation to maintain the secrecy of such information and are bound by the provisions of SF 312, "Classified Information Nondisclosure Agreement," and DD Form 1847-1, "Sensitive Compartmented Information Nondisclosure Statement." No additional facts, amplification, or comments shall be made about unauthorized disclosures of classified information.

5. FOREIGN DISCLOSURE. The provisions of this section shall not be waived.

a. All classified intelligence information intended for release outside the originating agency shall be explicitly marked with at least one of the authorized, mandatory foreign release markings (Releasable by Intelligence Disclosure Official (RELIDO), Releasable to (REL TO), or Not Releasable to Foreign Nationals (NOFORN)) or FOR DISPLAY ONLY to assist customers in information sharing.

b. SCI may be disclosed or released to foreign governments and international organizations in one of two ways:

(1) As SCI, in accordance with DCID 6/7 (Reference (p)), pursuant to a DNI-approved bilateral or multilateral agreement or arrangement; or

(2) As sanitized, or otherwise altered, SCI-derived information at the collateral level after approval by a duly authorized foreign disclosure officer in accordance with National Disclosure Policy (Reference (q)).

c. Reference (p) provides Intelligence Community policy and procedures for the disclosure and release of SCI and classified intelligence to foreign governments and international organizations, and coalition partners consisting of sovereign states.

(1) Disclosure or release of SCI beyond existing DNI policy guidance must be coordinated with the originator of the information and the Assistant DNI for Policy and Strategy.

(2) Any release of SCI to foreign governments must be approved by the SCI originator.

(3) SCI shall not be disclosed to other foreign entities without approval from the DNI, his designee, or the HICE, as appropriate.

(4) Release of SCI-related, unclassified technology is subject to export controls as established by the DoD, Department of State, and Department of Commerce.

6. PROTECTION OF SOURCES AND METHODS

a. DCID 6/6 (Reference (r)) establishes policy for the use of dissemination controls to maximize the dissemination of intelligence consistent with national security requirements and the need to protect sources and methods from unauthorized disclosure. Although dissemination controls are important tools in carrying out the DNI's statutory responsibilities to protect sources and methods, inappropriate use of such controls impedes efficient and timely access to intelligence information required to meet customer needs. Therefore, all IC organizations will apply dissemination controls judiciously to ensure the intelligence information is disseminated to those who need it without unnecessary restrictions.

b. Access to SCI is based on ICD 704 (Reference (s)) eligibility, need-to-know, formal access approval, and indoctrination. SCI will be disseminated at the lowest level of classification that will satisfy official requirements.

c. All DoD Components will ensure that the intelligence they produce and disseminate excludes, sanitizes, or generalizes in descending order of preference the source and method data. Producers of finished intelligence shall:

(1) Avoid publishing products that must be controlled in collection system compartments. When treatment of a particular subject in an intelligence product requires discussion of operationally compartmented sources and methods, a special supplement, appropriately controlled in compartmented channels, is the preferred approach.

(2) Ensure unavoidable references to intelligence sources or methods are as non-specific as practicable. Subject to the provisions of collection system manuals, generalized discussion of compartmented collection capabilities is permitted in finished intelligence products controlled in a product-oriented compartment. Discussion of collection gaps, capabilities to provide indications and warning intelligence, or advice on the reliability of sources in finished intelligence at a relatively low level of compartmentalization must not exceed allowable boundaries of SCI control and thereby risk exposure of particularly sensitive intelligence.

d. The policy constraint on the use of compartmented information regarding sources and methods in finished intelligence products applies to all DoD publications including formal and informal memorandums and studies.

7. STANDARD OPERATING PROCEDURE (SOPs). SCI security officials shall establish written SOPs as required for their individual operational environments. The SSO shall ensure that SOPs do not conflict with DNI, DoD, or Military Department regulatory guidance. The SSO for the facility to which the SOP applies and the contractor management official responsible for SCI shall review SOPs and forward to the SIO, Commander, delegated Component official, or corporate official for approval. The approving official shall thereafter review them annually and document the review in writing. SOPs shall be part of the security orientation for personnel assigned to the areas to which the SOPs apply.

8. POLICY WAIVERS

a. Except as otherwise stated, the HICEs may waive the provisions of this Manual under extraordinary circumstances. The HICE may delegate this authority to the CSA. Waivers will be issued for a specific period, usually 1 year, or as otherwise specified by the waiver. The requester must correct the situation covered by the waiver prior to the expiration date or request an extension of the waiver. The local SCI security official shall inform other agencies or services desiring to share the facility of the waiver condition. Exceptions to policy shall be kept on file in the SSO and in the field unit SCIF, as applicable.

b. Waivers for the physical or technical security of a SCIF shall be done in accordance with the procedures outlined in ICD 705 (Reference (t)) and Volume 2 of this Manual.

c. This Manual does NOT authorize the waiver of reporting requirements to law enforcement or counterintelligence agencies.

9. INSPECTIONS. DIA/DAC is the authority for DoD SCIF inspections. DAC is authorized to inspect periodically any DoD SCIF and direct action to correct any deficiency including removal of SCIF accreditation. A physical inspection shall be conducted prior to accreditation by DAC or its designee as part of the accreditation process. After accreditation, inspections will be conducted periodically and will be based on risk management principles. Inspections shall be conducted in accordance with Reference (t), this Manual, and any other applicable DoD issuances. At a minimum, the inspection will include SCI security policy and procedures, security administration, information security, personnel security, physical security, technical security, and IA.

a. Periodic inspections will be scheduled based on threat, sensitivity, physical modifications, and past security performance. Inspections may occur at any time, announced or unannounced. Additional inspections may be conducted in the event of suspected compromise or incidents, history of deficiencies, major facility modification, or change in threat level.

b. Authorized inspectors (See Glossary for definition) will be admitted to a SCIF without delay or hindrance. Government-owned inspection equipment will be admitted into a SCIF without delay.

c. Inspectors will submit a written report following each inspection identifying any deficiencies and corrective action to be taken. The report will be forwarded to appropriate SCI officials and a copy maintained within the inspected SCIF and by DAC. Joint users of the SCIF will accept the results of DIA security reviews for validation of security compliance. These written reports will be available to the DNI or designee upon request.

d. Staff assistance visits (SAVs) must be conducted to review security support actions and administrative inquiries, and to support program review and approval as deemed appropriate by the CSA. Any recommendations that affect physical security, TEMPEST, or technical security will be validated by DAC prior to corrective action or expenditure of funds. When a report is issued by an SCI security official, findings and corrective actions are subject to review during the next inspection.

e. SCI security officials shall conduct self-inspections of their SCIFs annually and will use the self-inspection checklist provided on the DIA/DAC Joint Worldwide Intelligence Communication System(JWICS) webpage at http://www.dia.ic.gov/homepage/da/security/field/scifforms.html. The purpose of the self-inspection is to ensure compliance with the policies and procedures contained in this Manual and other applicable SCI security regulations and directives. Self-inspections will be coordinated with the site IA manager (IAM) 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. SCI security officials will use the self-inspection checklist provided on the DIA/ DAC webpage at http://www.dia.smil.mil/homepage/da/security/field. Results of the inspections will be routed through the unit commander/COR to the Component SSO. SCI security officials must specify in writing all findings and corrective actions taken and retain the report until the next self-inspection. An annual summary of self-inspection findings and actions will be forwarded to DIA/DAC-2 by the Military Department CSAs and Component SIOs.

f. 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 Manual. Inspections by non-SCI indoctrinated entities is 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, etc. 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.

10. DIA COMPARTMENTED ADDRESS BOOK (CAB)

a. A CAB record contains the name of the organization, its major command, SCIF collateral mailing address, DCD address, DSSCS and GENSER plain language message addresses, contact information for the SCIF primary and alternate managers, and the security classification and compartments the SCIF is authorized to receive and maintain. CAB records also contain an area for the SSO to list all elements they support. The CAB record contains a large free text area for special instructions (such as how to pass clearances to the SSO) and another free text area for recording JPAS designations.

b. SSOs shall submit changes to the CAB as they occur to their HICE or Component SIO via message or e-mail.

c. The HICEs are authorized to appoint individuals in their immediate organization to directly make these validated changes to the CAB. Designations must be made via message to SSO DIA//EON-2A with the subject line CAB Validator Appointment.

11. IA. DIA Directive 8500.002 (Reference (u)) and ICD 503 (Reference (v)) contain the policy and procedures pertaining to automated IS security for SCI. The IA program was established to maintain the security of intelligence IS and data stored, transmitted, and processed on these systems. IA officials will coordinate with the SSO on matters concerning IS/network security as needed to provide full compliance with all applicable security directives.

ENCLOSURE 4

IS

1. ORIGINATOR AND CONTRACTOR RESPONSIBILITIES

a. Originators. The drafter of a document or other classified material is 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. Each individual is also responsible for ensuring SCI material is properly protected. All personnel who produce, transmit, reproduce, or extract SCI from documents or other materials must properly mark and protect the resulting SCI product. They shall protect all hard copies, soft copies, and other related media (including, but not limited to, computer disks and typewriter ribbons) in the same manner as the final material and shall report errors in classification and marking, control, or dissemination problems to the responsible SCI security official. In addition they shall:

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

(2) 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.

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

b. 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 COR, COTR, 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 Chapter 5 of DoD 5220.22-M (Reference (w)). This requirement must be included in item 13 or 14 of the DD Form 254. The information management system employed by the contractor shall be capable of facilitating such retrieval and disposition in an expeditious manner.

2. STANDARD CLASSIFICATION MARKINGS. Classification and control markings shall be applied explicitly and uniformly when creating, disseminating, and using classified and unclassified information to maximize information sharing while protecting sources, methods, and activities from unauthorized or unintentional disclosure. Documents containing SCI shall be marked in accordance with ICD 710 (Reference (x)). Standard classification markings are markings that indicate the level of classification; the source of classification (and for original

classification decisions, the reason for classification); the agency and office of origin; and downgrading and declassification instructions. Also included are warnings notices (if applicable); intelligence control markings; portion markings; and page markings.

a. Levels of Classification. There are three levels of classification: TOP SECRET, SECRET, and CONFIDENTIAL.

b. Authority for Classification. The classification authority designates the basis for classification and is either an original or derivative.

(1) Original Classification Authority (OCA). OCA is the initial determination that information could be expected to cause damage to national security if subjected to unauthorized disclosure. This decision shall be made only by OCAs who have been specifically delegated the authority to do so, have received training in the exercise of this authority, and have program responsibility or cognizance over the information. OCAs shall develop classification guides for subject matter under his or her cognizance. Original classification decisions made by an OCA should be recorded in a security classification guide.

(a) Reasons for Classifying. To be eligible for classification, information must fall within one or more of the categories of information listed in section 1.4. of Reference (l). The "Reason" line is only used on documents originally classified by an OCA.

(b) Duration of Classification. At the time of original classification, the OCA shall establish a specific date or event for declassification based upon the sensitivity of the national security information. Upon reaching the date or event, the information will automatically be declassified.

(2) Derivative Classification

(a) The marking of the newly developed information is consistent with the classification markings that apply to the originally classified source. This includes the classification of the information based on a security classification guide or source documents. The majority of classified information is produced by derivative classification. The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. The derivative classifier shall include the source list in or with all copies of the derivatively classified document.

(b) When preparing a new document from several classified documents, the marking will reflect the highest classification of information extracted from the various source documents.

3. MARKING DOCUMENTS. All classified information shall be clearly marked so as to leave no doubt as to the classification level, the reason for classification, the duration of classification, and the authority or source for classification. Proper markings are required for both hard copy and electronic classified documents. Guidance for the IC and DoD marking requirements and

the categories of classification and control markings can be found in Reference (k)), and the DNI CAPCO Authorized Classification and Control Markings Register (Reference (y)).

4. RESTRICTED DECLASSIFICATION VALUES AND CAVEATS

a. MANUAL REVIEW (MR). The use of "MR" as a declassification value is no longer authorized as specification of declassification values has been eliminated from the classification banner lines of national intelligence documents. The full textual description of the event, date for declassification, or authorized exemption must be specified in the Classification/Declassification block on the first page of the classified document as required by paragraph 3.c of this enclosure.

b. NOFORN

(1) The NOFORN caveat will only be applied to intelligence information in accordance with References (p) and (r). Only HICEs or OCAs in elements of the IC may determine what information warrants application of the NOFORN caveat. Derivative classifiers shall only use the caveat when authorized by security classification guides or other properly marked source documents.

(2) NOFORN shall not be applied to non-intelligence information unless explicitly allowed by a DoD level instruction.

5. RE-MARKING PREVIOUSLY CLASSIFIED MATERIALS. The re-marking of material classified under previous DoD issuances is not required. However, if such information is extracted from that material and placed in a new document or republished, it must be marked according to current requirements.

6. LETTERS OF TRANSMITTAL

a. Classified Letters of Transmittal. If the letter of transmittal itself contains classified information, mark the letter with the highest classification and all SCI codeword's, caveats, and control markings that appear on the letter or the enclosures. Include appropriate paragraph markings and classification blocks (i.e., the "Derived From" and "Declassify On" lines). Place the following notation above the classification line at the bottom of the first page of the letter: REGRADE AS (Insert classification, caveats/code words, and control markings as applicable to the transmittal letter/memorandum only.) WHEN SEPARATED FROM ENCLOSURE(S) AND UPON PHYSICAL REMOVAL OF APPROPRIATE SCI CAVEATS, CODEWORDS, AND CONTROL MARKINGS.

b. Unclassified Letters of Transmittal. If a letter of transmittal itself is unclassified but has one or more SCI enclosures, mark the letter with the highest classification and all SCI code words, caveats, and control markings of the enclosures or the letter. Place the following notation

above the classification line at the bottom of the first page of the letter: "REGRADE AS UNCLASSIFIED WHEN SEPARATED FROM ENCLOSURE(S) AND UPON PHYSICAL REMOVAL OF APPROPRIATE SCI CAVEATS, CODEWORDS, AND CONTROL MARKINGS."

c. When a letter of transmittal is separated from its enclosure, follow the regrading instructions on the letter and downgrade as appropriate.

7. WORKING MATERIALS

a. Date working materials when created and mark each page with the notation "Working Papers--Destroy Within 180 Days."

b. Mark with the highest classification of any information contained therein; safeguard working materials according to the handling, storage, and disposition requirements for non-accountable SCI documents as described in this enclosure.

c. When used informally as coordinating drafts or staff papers, such materials may be physically transported or electronically transmitted via a secure means between action officers without marking as required for finished documents.

8. SPECIALIZED MEDIA

a. Automated Information System (AIS) Media. Each media item (e.g. CDs, DVDs, hard disk drives, etc.) containing SCI will be externally labeled, as appropriate, with an SF 712 or other identifying color-coded markings in accordance with SF markings, to show its classification and SCI control system caveats. Internal AIS media identification will include security markings in a form suitable for the media (i.e., classification; SCI system caveats, and Reference (y) control markings, if applicable). The introduction and removal of media from an SCI environment will be accounted for by document control procedures. All removable hard drives must be controlled and handled according to SCI document control procedures.

b. Computer-to-Computer Transmissions. SCI material transmitted by SCI approved and accredited AIS systems is considered controlled while in softcopy format. Once the SCI data is output to hardcopy format, the printouts must be controlled as a hardcopy document.

c. Photographic Media

(1) Label or color code photography in roll, flat, digital memory card, or other form with its classification and SCI control system caveats or code words. For film in roll form, place the label on the end of the spool flange, on the side of the spool container, and on the container cover (if any). If the container and its cover are transparent, no label is needed if the flange label is visible through the container. The roll film will include head and tail sequences giving all security markings applicable to its contents.

(2) Mark positive film flats or slides with individual internal markings showing the classification and SCI and other control markings. Label the front and back of frames for slides and view graphs with the classification and required markings, which may be abbreviated if necessary to fit the space provided. When feasible, photographically burn the classification and caveats into the print, slide, or image, itself.

(3) Protect and process undeveloped, exposed film and imagery at the highest level of SCI security protection required by its contents.

d. Video Tapes, Digital Video Discs, or Movie Film. These media will contain the classification and control information at the beginning and end of the media presentation. Label containers as well as the media itself to show the title; date; security classification; SCI caveats, code words, and dissemination control markings; and classification authority block.

e. Microform, Microfiche, and Microfilm Media. Handle and control these media as a hardcopy document. Label containers as well as the media itself to show the title, date, security classification, SCI caveats and code words and dissemination control markings, and classification authority block.

f. Marking in the Electronic Environment

(1) Where special provisions for marking some types of computer-generated information are needed, identify as clearly as possible the information that requires protection and the level of protection it requires, and make available either on the item or by other means, the other required information.

(2) Classified information resident in an electronic environment is subject to all of the requirements of References (l) and (k) and shall be:

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

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

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

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

(3) All e-mail, blog and wiki entries, bulletin board posting, and other electronic messages shall be marked as finished documents, in accordance with the requirements of this enclosure.

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

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

g. Graphic Arts Material. Mark all visual aids to include Power Point slides, maps, artwork, blueprints, and such other material with the security classification and SCI control system or code words before the legend, title block, scale, bullets, and at the top and bottom in such a manner as to be reproduced on all copies. Classification authority and declassification instructions shall be on the first page of the graphic arts material.

9. FAX CONTROL PROCEDURES. The secure fax machine used within the SCIF must be approved and accredited for the appropriate classification and access level of the material processed. Individuals transmitting and receiving the material shall have the appropriate clearance, SCI accesses, and need to know.

a. SCI documents transmitted by secure fax shall be marked and controlled in the same manner as hardcopy documents.

b. Individual header or cover sheets used to precede the transmission of SCI material by secure fax shall be conspicuously marked with the highest security classification of the transmitted material and unclassified digraphs/trigraphs, handling caveats, and Reference (y) control markings. The cover sheet will include the originator's name, organization, and phone number; the subject in unclassified form; the number of pages; and the receiver's name, organization, and phone number.

10. COVER SHEETS. Cover sheets shall be used on SCI documents upon removal from security containers or SCIFs to guard against unauthorized disclosure. Cover sheets should also be used when an SCI document is not actively being used in an open storage environment.

Cover sheets shall show, by color, which SCI control system or combination of systems applies, the classification, and applicable markings. Cover sheets should use the appropriate unclassified digraphs and trigraphs instead of the SCI code words. Cover sheets shall never display classified information (e.g., code words, caveats). Use normal forms distribution channels to order SCI cover sheets . Local color reproduction and overprinting of cover sheets are permissible. SCI cover sheets can be downloaded from the DIA website at http://www.dia.ic.gov/homepage/security.html, provided there is color print capability.

11. SCI ACCOUNTABILITY

a. General. The use of document numbers and other similar systems to provide accountability for individual SCI documents as a security protection measure is no longer required except for material specifically designated as accountable SCI.

b. Non-Accountable SCI. SI, TK, and G material has been designated as non-accountable SCI. HCS material is non-accountable unless determined otherwise by the HCS Secretariat.

c. Accountable SCI. Accountable SCI is determined by the DNI or HICE to be of such critical sensitivity as to require the most stringent protection methods, including traceability and audit. The DNI or HICE shall approve such document accountability, in writing. This authority may not be delegated.

d. Inventories of Accountable SCI. HICE or their designee shall maintain the annual inventory of accountable SCI.

(1) All DoD Components will honor the designation of accountable SCI.

(2) An annual report of accountable authorizations, volume, and cost may be required at the request of the DNI.

(3) Accountability records are not required for non-accountable SCI. Intelligence information that has not yet been converted into finished intelligence is considered non-accountable SCI.

(a) Records for Incoming Accountable SCI. A record shall be kept of accountable SCI and shall identify the material by document accountability number and copy number, originator, and a brief description of the material and storage location. Keeping copies of receipts or maintaining other records that provide required identifying data satisfy this requirement. For electronic records, retention of standard telecommunications center records fulfill this requirement. Internal receipting or administrative controls within the same SCIF is not required.

(b) Records for Outgoing Accountable SCI. A receipt is required for accountable SCI. Receipts shall identify the material by accountability number, copy number, and originator, contain a brief unclassified description of the material and identify the recipient. The required

DCD pouch or package receipt kept by the sender is sufficient to fulfill this requirement. The originator is responsible for preparing receipts for SCI material.

(c) Records Retention. For accountable SCI (e.g., SAP material), retain records of incoming and outgoing accountable SCI (such as receipts and document control logs) and certificates of destruction as permanent records (see paragraph 19.b. of this Enclosure). For non-accountable SCI, transmission receipts may be destroyed on acknowledgment of successful transmission to the intended recipient.

12. SCI DOCUMENT ACCOUNTABILITY NUMBER

a. Assign an accountability number to accountable SCI material only. Accountability numbers are not required for SCI documents unless explicitly required by program specific guidance.

b. Assign copy numbers to individual documents. Place the copy number next to or near the control number at the lower right corner of the document. Show reproduced copies with a combination of digits and letters (e.g., Copy 1A, Copy 4C) or identify the copy as Series B, Series C, etc.

c. The HICE or designee may designate special control numbers for contractor-originated SCI.

13. STORAGE. SCI material shall be maintained and stored in an accredited SCIF.

a. Combinations and codes to access control devices should be given to a limited number of SCI-indoctrinated personnel consistent with effective SCIF operations. Combinations to locks installed on security containers, perimeter doors, and any other openings must be changed:

(1) When a combination is first installed or used.

(2) When a combination has been compromised, or believed to have been compromised.

(3) At other times when considered necessary by the SSO.

(4) When taken out of service; combination locks shall be reset to the standard combination 50-25-50.

b. Codes to access control devices (cipher, electronic, etc.) shall be provided only to SCI indoctrinated personnel.

c. When practical, SCI material should be segregated from other material in a separate file cabinet, drawer, or folder. Security regulations or directives governing collateral files do not apply to SCI material.

d. U.S. collateral classified information used in a SCIF shall be stored in accordance with the SCIF accreditation and managed in accordance with the guidance in Reference (k).

14. TEMPORARY RELEASE OUTSIDE OF A SCIF. In Government facilities, when operational needs require the release of SCI for temporary use by SCI-indoctrinated persons in non-SCI accredited areas, only the CSA, their designee, or the Component SIO may grant such release. In a combat zone, the force commander or local SIO may authorize temporary release under emergency conditions. The SCI security official shall obtain a signed receipt for SCI released in this manner and ensure that conditions of use of the released material provide adequate security to include acoustic and visual protection until the SCI is returned to a SCIF by the end of the duty day. SCI material shall not be left with non-SCI-indoctrinated personnel. This does not preclude transporting of properly wrapped SCI by DCD or U.S. Diplomatic Courier Service personnel. If temporary release is needed for more than one or two occasions, consideration should be given to establishing a permanent SCIF. This temporary release authority is not intended to remove the requirement to use a properly accredited SCIF in day to day situations.

15. REPRODUCTION. Reproduction of SCI documents shall be kept to a minimum consistent with operational necessity. Within a SCIF, reproduction equipment must display the classification levels and SCI authorized for reproduction by each piece of reproduction equipment.

a. Stated prohibitions or limitations against reproduction shall be honored. The originator is the approval authority for reproduction in such cases.

b. Copies of documents are subject to the same control, accountability, and destruction procedures as the original documents. Extracts of documents shall be marked according to content and treated as working materials.

c. Equipment connected to remote diagnostic centers, such as by telephone lines, are prohibited for SCI reproduction unless the capability has been disabled.

16. TRANSPORTATION OF SCI INFORMATION

a. General Provisions. Alternately, SCI shall be transferred by SCI indoctrinated persons, certified or designated couriers, diplomatic pouch, or DCD. The SSO or SCI Security Official shall establish strict accountability and control for courier cards.

(1) The preferred method of transporting SCI from one SCIF to another shall be via secure e-mail or other secure electronic means. Alternatively, SCI shall be transported by SCI-indoctrinated persons, certified or designated couriers, diplomatic pouch, or DCD. See section 17 of this enclosure for specific wrapping instructions.

(2) When transporting SCI within a single building (military headquarters or DoD-controlled building), SCI material shall 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. The briefcase or pouch shall bear a subtle notice indicating that anyone finding the container unattended must notify the owner immediately and to arrange to return it unopened to the owner. Formal designation or identification of a courier is not required.

(3) When transporting SCI between SCIFs in two different locations (different buildings or different bases), in addition to the requirement in subparagraph 17.a.(1) of this enclosure, an inventory of the contents shall be left in the departure SCIF until proof that the SCI has arrived at the destination. Formal designation or identification of a courier is required.

(4) Couriers traveling aboard U.S.-flag commercial aircraft must also have a separate signed original letter of authorization as shown in Appendix 1 to this enclosure, and as required by the Transportation Security Administration and Federal Aviation Administration. Coordinate with airport security officials prior to travel whenever possible.

(5) Couriers must have a DD Form 2501, "Courier Authorization," or equivalent with the acronym "SCI" displayed prominently on one portion of the card.

b. Courier Authorizations

(1) If electronic transmittal of SCI is not possible, and hand-carrying SCI will occur within the United States, SSOs shall appoint couriers in writing. SSOs may approve hand-carrying of SCI aboard U.S.-flag commercial passenger aircraft for travel within the United States.

(2) For travel outside the United States, the local SIO shall appoint SCI couriers in writing. SIOs may delegate this authority to SSOs, except for couriering on foreign-flag aircraft.

(3) Air Courier Orders are not required for transport of SCI material via military aircraft (such as the Air Mobility Command).

(4) SCI couriers may transport collateral classified material without a separate designation as a collateral courier.

(5) The appointing authority shall maintain a current list of all designated couriers.

(6) Travel orders will not indicate that the individual is an SCI courier, but may show "Official Courier." Instructions applicable to the local situation may be added.

(7) The SSO or SCI security official shall establish strict accountability and control for courier cards.

c. Courier Requirements. Couriers shall be an active duty military person, including reservists on active duty for training and Federalized National Guardsmen; a U.S. Government

civilian employee; or a DoD contractor (when authorized by DD 254 or consultant (when authorized by statement of work order). Couriers shall be specifically designated as a courier, and have authorized access to the SCI material they are transporting. They 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. SCI material shall be properly wrapped prior to giving the material to a courier except when paragraph 17.a.(2) applies.

(1) Certified couriers are individuals whose primary responsibility is to courier SCI material worldwide.

(2) Designated couriers are individuals whose temporary responsibility is to courier SCI material.

(3) Prior to receiving a courier card, each courier shall read the appropriate extracts from the espionage laws and execute a certificate acknowledging receipt of the courier card. See Appendix 2 of this Enclosure for the certificate format.

d. Courier Procedures. The local SIO shall establish courier procedures for organizations under their security cognizance. The procedures will reflect the policies and procedures of this Volume, will designate local travel areas; will ensure SCI materials are handled only by SCI indoctrinated individuals; will ensure the materials are protected against the possibility of hijacking, loss, exposure to unauthorized persons, or other forms of compromise; and will ensure courier procedures comply with Transportation Security Administration policy.

(1) General. One person may serve as a courier; however, the courier authority shall assess the circumstances such as volume of material, means of travel, high crime area, or sensitivity level and determine if more than one person is required to maintain continuous custody of the material. DIA recommends using two SCI-indoctrinated personnel couriers beyond the local travel area because of the possibility of emergency situations.

(a) The SCI storage provisions of this Manual apply at all stops en route to the destination, unless the SCI is retained in the personal possession of the courier, and under constant surveillance at all times.

(b) Hand-carrying SCI on trips that involve an overnight stop is not permissible without advance arrangements for secure overnight storage of the SCI in a U.S. Government facility which is accredited to store SCI. Within the United States, a cleared contractor facility that has the requisite storage capability may be used.

(c) SCI shall not be read, studied, displayed, discussed, or used in any manner in public conveyances or places.

(d) SCI shall not be hand-carried across international borders unless the home station activity issuing the written authorization is relatively certain that the SCI will not be opened by foreign customs, border, postal or other inspectors, either U.S. or foreign.

(e) Envelopes containing SCI shall not be used to carry or convey personal items, communications, or other similar objects.

(f) Round trip hand-carrying of SCI is the exception rather than the rule. If the SCI is to be returned to the home station, it should be transmitted back from the travel destination by secure means.

(2) Ground Transportation. See Appendix 3 to this Enclosure for specific instructions.

(3) Air Travel.

(a) Authorization to hand-carry SCI on a plane may be granted only in exceptional situations and when:

1. The material is needed urgently for a specified official purpose; and

2. There is a specified reason that the material could not be transmitted by other approved means in enough time for the stated purpose.

(b) Couriers shall possess an original letter of authorization for commercial air (see Appendix 1 to this Enclosure), shall receive written special instructions (see Appendix 3 to this Enclosure), and shall sign a statement acknowledging understanding and acceptance of courier responsibilities.

(c) Recurring or blanket courier letters of authorization for commercial air will not be issued.

(d) Couriers shall use foreign carriers only when no U.S.-flag carrier is available. The approving official must ensure that the SCI will remain in the custody and physical control of the U.S. courier at all times. Authorization will be granted on a case-by-case basis and only when all efforts to transmit by other means is not possible.

(e) Envelopes containing SCI are to be free of metal binders, clips, or other metallic objects that might trigger air terminal screening devices. If the envelopes are in a briefcase or carry-on-luggage, the briefcase or luggage may be opened for inspection. The screening officials may check envelopes by x-ray machine, flexing, feeling, and weighing.

(f) Shipping SCI in cartons or containers too large to hand-carry aboard commercial passenger aircraft is highly discouraged. If the SCI cannot be kept in the possession of the courier at all times, it should be shipped via DCD.

(g) If the transport of cargo is approved aboard military, U.S. chartered aircraft, or commercial airlines, the actual loading and unloading of the SCI will be under the supervision of a representative of the air carrier. The appointed courier shall accompany the classified cargo and keep it under surveillance during loading and unloading operations. In addition, appropriately cleared personnel (to include the courier) must be available to conduct surveillance

at any intermediate stops where the cargo compartment is opened. These arrangements require prior coordination with the airlines and the Transportation Security Administration.

(4) Issuing Courier Letters to Non-Assigned Personnel. Local SCI security officials may issue courier letters of authorization to non-assigned personnel to hand-carry SCI when:

(a) The local SCI security official verifies the individual and the receiving facility has the appropriate clearance and access level. The verification may be made by the personnel security system of record or telephone.

(b) The parent or supporting SCI security office confirms the requirement for the individual to courier the material. The confirmation may be made by telephone.

(c) The local SCI security official packages the material and prepares the proper receipts and inventory list.

17. SCI WRAPPING REQUIREMENTS

a. SCI requires double-wrapping using two opaque envelopes, Kraft wrapping paper, or canvas bags, cartons, leather or plastic pouches, or similar containers which preclude observation of the contents. Seal all seams of both wrappers with reinforced paper tape or utilize tamper-evident tape or tamper-evident containers/bags. Do not use masking or cellophane tape. Retain an inventory of the material until verification is received that the information was delivered to an authorized recipient. Prepare packages for distribution as described in this section. If project or control officer material requires special procedures, follow the project office guidelines.

(1) Inner Wrapper

(a) Place the address of the receiving SCIF in the center of the package; place the address of the sending SCIF in the upper left corner.

(b) Include originator package control number if applicable (lower right corner is recommended).

(c) Stamp or print in large letters above the address of the receiving SCIF: "TO BE OPENED ONLY BY (SCI security official, e.g., SSO, GAMMA control officer, TCO, HCO, or appropriately cleared recipient)."

(d) Stamp or print in large letters at the top and bottom on each side, the appropriate security classification and SCI compartments.

(e) Stamp or print the statement: "CONTAINS SENSITIVE COMPARTMENTED INFORMATION" on each side.

(2) Outer Wrapper

(a) Place the address of the receiving SCIF in the center of the package; place the address of the sending SCIF in the upper left corner.

(b) Include the originator package control number, if used (lower right corner is recommended).

(c) Secure outer containers with tape, lead seals, tumbler padlocks, or other means which reasonably protect against surreptitious access.

(d) DCD packages have special outer-wrapper instructions. Refer to the U.S. Transportation Command Website (http://www.transcom.mil/dcd) for detailed instructions.

b. SCI shall be transported from one SCIF to another in a manner that properly protects the SCI material. For local travel, SCI material may be hand-carried using a locked pouch as the outer wrapper along with an inner wrapper. Attach an unobtrusive luggage tag with the following notation to the pouch: "PROPERTY OF THE U.S. GOVERNMENT TO BE RETURNED UNOPENED TO (name of the appropriate organization and telephone number that will be manned at all times)."

c. Special Wrapping Requirements

(1) If the classified portion of an SCI project is an internal component of a piece of equipment or other bulky item whose outside shell is not classified and completely shields the classified aspects of the item from view, the shell may serve as the outer covering.

(2) If the classified portion of the SCI material is an item of equipment that cannot easily be put into a packaged and the shell or body is classified or sight-sensitive, drape the equipment with an opaque covering that will conceal all classified or sight-sensitive features. Coverings must be secured to prevent accidental exposure of the item.

(3) Specialized shipping containers, including closed cargo transporters, may be used in lieu of the package requirements described in paragraph 17.a. of this enclosure and may serve as the outer wrapping.

(4) Packaging material shall be strong enough to provide protection while in transit and to prevent damage or compromise of classified material or information. Use seals, Kraft paper, reinforced tapes, puncture resistant material, wire mesh or other knife-slashing resistant material to prevent items from breaking out and to facilitate the detection of tampering. The inner contents, labels, tags, etc., shall not be visible.

18. DISPOSITION

a. Contractors shall return all classified material received or generated in the performance of a classified contract unless the material has been approved for destruction by the Government, or the DD Form 254 or other official document(s) authorizes retention.

b. SCI shall be retained for the time periods specified in records control schedules approved by the archivist of the United States in accordance with section 3302 of title 44, U.S.C. (Reference (aa)). Destroy duplicate and non-record copies of SCI documents as soon as their purpose has been served.

19. DESTRUCTION

a. Destroy SCI in a manner that will prevent reconstruction. Only those DNI approved methods (e.g., burning, pulping, shredding, pulverizing, melting, or chemical decomposition, depending on the type of materials to be destroyed) specifically authorized by the responsible SIO may be used. SCI indoctrinated person(s) will conduct the destruction. The SIO or designee may determine that two persons are appropriate when high volume or bulk destruction of accountable data or when the destruction of accountable data is external to a SCIF. SCI in computer, AIS, or other computer storage media will be destroyed as specified in NSA/CSS policy.

b. Destruction certificates are required for accountable SCI. If an organization maintains a master record of accountable SCI and destruction is recorded in the master record, individual destruction certificates may be destroyed after recording in the master record. Multimedia copies of accountable records are authorized provided all information is readable and hardcopy prints can be made to meet investigative or judicial requirements.

c. SCI in computer or AIS or other magnetic media shall be destroyed as specified in the "Guide to Understanding Data Remanence in Automated Information Systems" (Reference (ab)), or as authorized by NSA in other publications.

d. If burn bags are used to hold SCI waste, mark the bag when placed in use with the highest security classification of the material it might contain, the phrase "CONTAINS SCI MATERIAL," and the office symbol and phone number of the SCIF. When filled, seal the bag with staples or tape to prevent accidental tearing or breaking. In SCIFs not accredited for open storage, SCI waste must be secured in approved GSA security containers.

20. EMERGENCY PLANS. Plans shall be developed to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action to minimize the risk of compromise, and for the recovery of classified information, if necessary, following such events. The level of detail and the amount of testing and rehearsal of these plans shall be determined by assessing the risk of hostile action, foreign intelligence threats, natural disaster, or terrorist activity that may place the information in jeopardy.

a. Use the requirements of Committee on National Security Systems Instruction 4004.1 (Reference (ac)) when developing plans for the emergency protection (including emergency destruction under no-notice conditions) of classified COMSEC material.

b. When preparing emergency plans, consider:

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

(2) Storing less frequently used classified material at other secure locations.

(3) Creating regular backup copies of information in electronic formats for off-site storage.

(4) Transferring as much retained classified information to removable electronic media as possible, thereby reducing its bulk.

Appendixes

1. Template for SCI Courier Letter of Authorization for Commercial Air
2. SCI Courier Certification
3. Special Instructions for One-Time Couriers of SCI Outside the Local Travel Area

APPENDIX 1 TO ENCLOSURE 4

TEMPLATE FOR SCI COURIER LETTER OF AUTHORIZATION FOR COMMERICAL AIR

SCI courier letters for commercial air travel should follow the template indicated in Figure 1 of this Appendix.

Figure 1. Template for SCI Courier Letter for Commercial Air

Letterhead Date

TO: WHOM IT MAY CONCERN

SUBJECT: One-Time Courier Letter of Authorization

1. This letter certifies that the person whose name appears below and whose identity may be verified by the credentials described is:

a. A member of the (name of the organization), Department of Defense, United States of America.

b. An official courier or escort for the (name of the organization).

c. Required to (escort or hand-carry) the (parcel or carton/container) as described from (original location) to the destination(s) shown (add "and return to (original location)." if round trip hand carrying is requested).

2. Name, Grade, and Service of courier: (e.g., DOE, John R., GS-14, Department of Defense civilian or DOE, John R., Major, U.S. Army, etc.)

3. Identification: (e.g., U.S. passport number, Armed Forces of the United States Identification Card number; or other DoD picture credential. If the identification does not contain the escort or courier's date of birth, height, weight or signature, those items must be included in this paragraph. Forms can be obtained at http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.)

4. Destination to include transfer points and date(s): (e.g., Washington, DC non-stop to New York City, NY, 2 July 2005 or Washington, DC via New York City, NY 1 July 2005 to Frankfurt, GE, 2 July 2005. Return from Frankfurt non-stop to Washington, DC, 5 July 2005. DO NOT LIST FLIGHT NUMBERS.)

5. Description of parcel or carton/container: (e.g., one (1) sealed envelope addressed to: CDR, USAREUR, ATTN: AERP, APO NY 09407; from DIA, ATTN: DAC-2A4, Wash, DC 20340, in a locked briefcase; or two (2) cartons, 12' x 12' x 12', addressed to: CDR, USAREUR, ATTN: AERP, APO NY 09407 from DIA ATTN: DAC-2A4, Wash DC 20340-1251).

APPENDIX 2 TO ENCLOSURE 4

SCI COURIER CERTIFICATION

1. Upon receipt of a DoD courier card or other document authorizing courier of classified information, the designated courier must execute a courier certification statement. The statement should include, at a minimum that:

a. The courier has received a briefing regarding the policy and procedures for couriering collateral or SCI material.

b. The courier fully understands and will comply with the responsibilities and procedures outlined in Reference (k) and other applicable information security policies for couriering classified information.

c. The courier will not divulge to unauthorized personnel the fact that they are transporting classified material.

d. The courier is fully aware that it is their responsibility to fully protect all material in their custody, against loss or compromise.

2. SCI courier certification should be signed by the courier and witnessed and signed by the security official issuing the courier order. A copy of this certification shall be maintained by the local security officer and destroyed 1 year after the expiration of the courier authorization.

APPENDIX 3 TO ENCLOSURE 4

SPECIAL INSTRUCTIONS FOR ONE-TIME COURIERS OF SCI OUTSIDE THE LOCAL TRAVEL AREA

1. SCI couriers are responsible for the protection of the material in their custody. Couriers must avoid all places, situations, and circumstances that could compromise their ability to protect the classified material. Couriers have discharged their responsibilities once they have released the material to the authorized recipient in the SSO at their destination.

2. All SCI materials shall be double-wrapped. A locked briefcase or pouch should serve as the outer wrapper. Attach a courier tag to the outer envelope of each parcel containing classified information. Do not attach a courier tag to the outside of a briefcase, attaché case, etc., or to a carton or container being escorted, as this would draw attention to the classified material. The inner wrappers must be marked or labeled as indicated in Figure 2:

Figure 2. Marking Inner Wrappers of Classified Material.

IF FOUND, DO NOT OPEN. IMMEDIATELY NOTIFY: SSO (name of organization and mailing address) Telephone: Defense Switched Network: After Duty Hours Telephone:

3. Opaque envelopes or wrapping paper, or tamper-evident packaging shall be used for the inner wrappers; all seams are to be taped with reinforced paper/plastic tape or tamper-evident tape. Bulky material may be packaged in durable fiberboard, cardboard, or wooden boxes. Place proper security classification and SCI caveats on both sides of the innermost wrapper. A list of all SCI material being transported must be left at the originating facility with the office of the courier. SCI documents will not be left with or signed over to another individual other than the specific addressee or the SSO.

4. SCI material shall remain in the courier's personal possession and under their constant surveillance at all times. The SCI must be stored in properly accredited SCIFs at all stops en route to the final destination. Do not leave SCI material in locked automobiles, quarters, hotel rooms, train compartments, etc., or stored in automobile trunks or in any detachable storage compartment. If intermittent stops are made between the origin of flight and final destination, the courier will witness the opening and closing of the storage compartment at each stop to make sure that the material is not tampered with or erroneously off loaded. To maintain custody of the material at an en route stop, the courier may place the material in the temporary custody of the local DCD station commander.

5. The shipping of SCI in cartons and containers that are too large to hand-carry aboard commercial passenger aircraft and must be placed in the aircraft's sealed cargo compartment is highly discouraged. If the SCI cannot be kept in the possession of the courier at all times, then it should be shipped via DCD on military air. If the transport is approved, the SSO who has authorized the transport of the SCI will notify the appropriate air carrier in advance. The courier will report to the affected airline ticket counter before boarding, present his/her documentation, and the package or cartons to be exempt from screening. The airline representative will review the documentation and description of the containers to be exempt. If satisfied with the identification of the courier and his documentation, the official will provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the container from physical or other type inspection. The actual loading and unloading of the SCI will be under the supervision of a representative of the air carrier; however, appropriately cleared personnel will accompany the classified information and keep it under surveillance during loading and unloading operations. In addition, appropriately cleared personnel (to include the courier) must be available to conduct surveillance at any intermediate stops where the cargo compartment is to be opened. If the airline official is not satisfied with the identification of the passenger or the authenticity of his documentation, the courier will not be permitted to board, and not be subject to further screening for boarding purposes. These types of arrangements require prior coordination with the airlines.

6. SCI hand-carried aboard commercial passenger airlines must be accomplished only aboard a U.S. carrier. Foreign carriers will be used only when no U.S. carrier is available. If a foreign carrier is used, the information must remain in the custody and physical control of the U.S. courier at all times.

7. Couriers shall use the most direct route feasible. If a courier is unable to follow the itinerary or if the material is lost, stolen, or otherwise subjected to compromise en route, the courier will immediately report the circumstances to the parent SSO. Hand-carrying SCI on trips that involve an overnight stop is not permissible without advance arrangements for secure overnight storage in a U.S. Government facility that is accredited to store SCI. Within the United States, a cleared contractor SCIF that has the requisite storage capability may be used. If an overnight stop or unforeseen delay is encountered while en route and an accredited facility is not available, the material may be stored at a DCD courier transfer station (CTS), if available. If a CTS is used for overnight storage, a signed receipt will be obtained. If none of these facilities is available, the courier must retain the material in their personal possession and properly safeguard it during the period of delay.

8. SCI will not be read, studied, displayed, discussed, or used in any manner in public conveyances or places. Do not discuss SCI except in secure areas officially approved for such discussion. All personnel having access to or viewing the material must be authorized the appropriate level of SCI access.

9. SCI documents must be returned to SSO control as soon as possible. Local couriers must return material to SSO control prior to the close of business on the day of receipt unless prior arrangements are made. Couriers will verify each item by the package, pouch, or, in the case of individual documents, control number when receipting for or delivering material. SCI material

will be delivered only to the specific addressees designated by the dispatching unit. Positive identification will be obtained before release of the material. Couriers will neither reproduce nor permit reproduction of SCI material without prior approval of (organization SSO).

10. SCI shall not be hand-carried across international borders unless the home station activity issuing the written authorization is reasonably certain that the SCI will not be opened by foreign customs, border, postal or other inspectors, either U.S. or foreign.

11. Envelopes containing SCI should not be used to carry or convey personal items, communications, or other similar objects.

12. Round trip hand-carrying of SCI is the exception rather than the rule. If the SCI is to be returned to the home station, it should be transmitted back from the travel destination by secure means.

13. SCI material shall be stored with a servicing SSO at the TDY location and provided to that SSO for wrapping, controlling and shipping by DCD to (home station). If material must be transported round-trip, the SSO at the TDY location will wrap and control material before remanding to the courier's custody.

14. Federal Aviation Regulations require that all passengers and their carry-on items be screened before boarding military or commercial aircraft. Couriers of SCI should routinely offer briefcases or pouches for inspection. The courier letter or order may be offered, if requested. The contents of briefcases and pouches may be allowed to go through metal detection devices unopened. In the event that the person conducting the screening is not satisfied, and there is doubt as to the contents of the envelopes, the courier will not be permitted to board with the briefcases or pouches. Never allow screening personnel to open envelopes containing classified material. Envelopes containing SCI must be free of metal binders, clips, or other metallic objects that might trigger air terminal screening devices. If the envelopes are contained in a briefcase or carry-on-luggage, the briefcase or luggage may be opened for inspection for weapons or contraband. The screening officials may check envelopes by x-ray machine, flexing, feel, and weight. In the event that the courier is not allowed to board the aircraft, they shall contact the authorizing SSO for instructions.

15. The courier appointment does not authorize the bearer to carry SCI material to their home or office for personal convenience. Recurring or blanket courier letters for commercial air are not authorized. Local SCI security officials shall not grant authority to non-assigned personnel to hand-carry SCI without prior permission of their parent agency, organization, service, or unit.

16. Noncompliance with the foregoing may be grounds for disciplinary action.

ENCLOSURE 5

TRANSMISSION SECURITY

1. ELECTRONIC TRANSMISSION OF SCI. Senders transmitting SCI electronically (including facsimile, computer, secure voice, e-mail, or any other means of telecommunication) must ensure that such transmissions are made only to authorized recipients. Recipients will provide proper protection for SCI received. Electronic transmission of SCI is limited to specifically designated and accredited communications circuits secured by an NSA-approved cryptographic system or a protected distribution system accredited in accordance with Enclosure 4 of Volume 2.

a. SCI, regardless of its classification, shall not be processed on, transferred to, or stored on SIPRNET-connected or unclassified information systems.

b. Any transfer to and/or processing or storage of SCI on SIPRNET or an unclassified system constitutes an unauthorized disclosure and must be reported in accordance with those procedures. The SSO shall contact and work with the information assurance staff to ensure appropriate and timely resolution of the incident.

2. SECURITY RESPONSIBILITIES. The local SSO is responsible for ensuring that supporting communications centers establish and implement appropriate security and control procedures to protect the categories of SCI and that all personnel are familiar with these procedures. Individuals are responsible for ensuring that message addressees are authorized to receive the category of SCI or multiple control system information to be transmitted. Any variation from the prescribed security standards for transmission of SCI by electrical means will be referred to SSO DIA/DAC.

3. COMSEC TRAINING PROGRAMS. Only properly trained individuals are authorized to operate cryptographic equipment. The DoD Components will ensure that personnel in cryptographic operations, maintenance, and other COMSEC specialties receive the required training to perform their duties.

4. GUIDELINES. The following is the minimum criteria for an electrical circuit transmitting SCI:

a. A circuit (not including an NSA-sponsored circuit) between two or more SCI facilities, except for Protected Distribution Systems (PDSs), must be validated by DIA in accordance with Department of the Interior Acquisition Regulation 35-2 (Reference (ad)). Retain the circuit validation documentation within the SCIF for which it was validated.

b. SCIFs must be accredited to the same level of SCI transmitted or received on electrical circuits entering or exiting the SCIF. The construction and protection of SCI

telecommunications facilities will be in accordance with Reference (t) and NACSI 4000-series or successor publications.

c. Personnel having access to the SCI unencrypted data on the circuit or personnel responsible for SCI encryption equipment must be SCI-indoctrinated to the appropriate level to minimize risk while still only granting access to sensitive programs when appropriate.

d. All equipment and associated transmission lines at each end of the circuit handling plain text (unencrypted) SCI must be installed in accredited SCI facilities. (The term "equipment" as used in this paragraph refers to all electrical and electromechanical devices used to handle plain text information, including but not limited to end-terminal equipment, patches, interface units, automated switches, multiplexers, and computer systems.)

e. COMSEC equipment and cryptographic systems must be NSA-approved for the highest level of classification of the traffic transmitted on the system.

f. All equipment, including COMSEC, and associated unencrypted transmission lines must be installed in accordance with Reference (m).

g. All equipment and PDSs must be accredited in accordance with Enclosure 4 of Volume 2.

5. COLLATERAL CIRCUITS WITHIN SCI AREAS. Communications, command and control, or intelligence data circuits that are not approved for the transmission of SCI will not be installed within a SCIF without the consent of the SCIF IA approval authority in accordance with section 6 of this enclosure. Additionally, such systems must be installed in a manner that preserves the communications and physical security integrity of collocated SCI systems and circuits and meets TEMPEST requirements.

6. APPROVAL AUTHORITY

a. The HICEs of the Military Departments and Command Level SIOs or CSAs, following the guidelines in section 4 of this enclosure, may authorize installation of collateral circuits in SCI facilities under their security cognizance. DAC shall be notified of all collateral circuits installed in SCIFs.

b. The HICEs of the Military Departments and Command Level SIOs and CSAs may grant temporary approval to transmit SCI over a circuit or protected distribution system. This approval shall be documented in writing with a signature. DIA may further delegate temporary approval authority for DoD Field Activities. Prior to granting interim approval, the approving authority must assess the risk and measures taken to manage the risk. Temporary approval shall not exceed 30 days; operational restrictions will be imposed as required. All circuits containing residual SCI (e.g., hard drives, routers, key material) must be properly secured in an accredited SCIF or continuously protected by SCI personnel when not in use. Commanders will notify DAC of interim approvals.

7. MULTI-FUNCTION OFFICE MACHINES (M-FOMs). M-FOMs are devices that have the capability to copy, print, scan, and fax, either in a standalone or networked mode. When connected to a network, M-FOM devices assume the highest classification for which the network is accredited. If operated as a standalone or multi-function device, these devices assume the highest classification of copied documents. Many M-FOM hard drives are capable of holding thousands of images depending on the size and complexity of the images. The SSO shall establish written procedures to protect the information contained within the hard drive and printed circuit boards/memory boards of the M-FOM.

a. All external data connections must be disabled when M-FOMs are used to process (i.e., scan, copy, print, or fax) classified information. Some M-FOMs have the capability to allow the vendor to receive copies of documents (i.e., 1 of every 100), through hardware or wireless transmission mediums, whether scanned, printed, copied or faxed, to maintain quality control of the M-FOM; these features must be disconnected or disabled.

b. To prevent the inadvertent or deliberate downloading of classified information, service technicians shall not connect a proprietary laptop to an M-FOM that processes classified information. Laptops required for diagnostics must be purchased by the command or agency (software included) and maintained by the SSO in the SCIF. The hard drive, printed circuit boards or memory boards, and like memory storage devices, cannot be removed from the SCIF to a non-SCIF area unless the device is properly sanitized of all classified or sensitive information. The classified information stored on the hard drive is the property of the United States and must not be released outside official channels. For this reason, all M-FOM hard drives and printed circuit boards or memory boards (Government or lease) must be removed prior to their final disposition.

c. Purchased M-FOMs are Government property. Turning them into the Defense Reutilization Management Office without a hard drive is acceptable, provided all printed circuit boards or memory boards are removed. Leased M-FOMs may need to be returned in working order at the conclusion of the lease. In this instance, a second hard drive should be purchased. The built-in internal hard drive may be extremely difficult to access and remove, requiring disassembly. For this reason, leasing the M-FOM with a removable hard drive vice an internal fixed hard drive is recommended. Printed circuit cards or memory boards will be removed prior to returning the M-FOM to the vendor.

d. Removal or return of purely mechanical or electro-mechanical parts to a vendor will only be permitted based on a risk determination that includes consideration of threat, vulnerability, impact, and cost. Printed circuit boards or memory boards are to be destroyed as classified trash at the classification level as determined in this enclosure. No parts will be released outside the United States or in areas with a high foreign intelligence or terrorist threat.

e. All communications ports not specifically required for networked or contractual maintenance must be removed or permanently disabled. Only hardwired connections are permitted. IR, RF, video, or audio communications are prohibited. This provision must be included in the purchase contract.

8. SECURE TELEPHONE DEVICES

a. In accordance with DoDI 8560.01 (Reference (ae)), all telephones subject to COMSEC monitoring will display DD Form 2056, "Telephone Monitoring Notification Decal."

b. The Crypto-Ignition Key for a Secure Telephone Unit (STU) III telephone or a Fortezza Card/KOV-14 for a Secure Terminal Equipment (STE) telephone located in SCIFs is configured by the NSA Electronic Key Management System Central Facility. Secure telephones configured with a TOP SECRET SCI key shall not be used in non-SCI accredited areas.

c. Telephones configured with a residential or mobile key can provide a limited capability for senior leaders and decision makers to receive secure calls. In these instances, security procedures covered in NSTISSI 3030 (Reference (af)) (for STE telephones) and NSTISSI 3013 (Reference (ag)) (for STU telephones) apply. Specific questions can be addressed to the supporting COMSEC officer or the National Security Agency, Information Assurance Policy, Procedures, and Insecurities Division (I41), (410) 854-6831.

ENCLOSURE 6

IS SECURITY

1. GENERAL. Reference (v) establishes the security policy and procedures for storing, processing, and communicating classified intelligence information in IC. The IC seeks standardization of IS security policy and procedures. The physical, personnel, and information security practices and procedures described in this Manual must accommodate a wide range of information system security concepts and requirements. Information system security and the achievement of information assurance are linked with and dependent upon all other security disciplines.

a. All DoD Intelligence Information Systems (DoDIIS) must be certified and accredited in accordance with References (u), (v), and this Manual. Joint Air Force-Army-Navy (JAFANs) regulations for SAP may also pertain to certain IS.

b. Unclassified or collateral (non-SCI) networked IS collocated in DIA SCIFs will be considered guest systems and their currently approved accreditation accepted. SCI security personnel will ensure IS security policies are in place to provide a continued safe SCIF IS operating environment and establish a mechanism for the SCI IA approval authority for these actions. SSOs and security personnel should reference other guidance as required such as ~~DoDD 8500.01E (Reference (ah)), and DoDIs 8500.2~~ *DoDIs 8500.01* and 8510.01 (References *(ah) and* (ai)~~ and (aj)~~).

c. All DoD IS must maintain an appropriate level of integrity, authentication, non-repudiation, availability, and confidentiality.

d. As the information system conditions and features are designed and implemented, it is important to consider:

(1) The importance and sensitivity of the information and information assets.

(2) Documented threats and vulnerabilities.

(3) The trustworthiness of users and interconnecting systems.

(4) The impact of impairment or destruction to the DoD information system.

(5) Cost effectiveness of security features or selected countermeasures.

e. Every DoDIIS must be accredited, either as a separately accredited system, or as part of an accredited DoDIIS site. Operation of stand-alone IS systems within SCIFs will be approved and accredited by the SIO.

2. SSO RESPONSIBILITIES. An SSO is responsible for all resident SCI information, including that which exists on IS within a SCIF. The SSO must coordinate IS security with the IAM. The IAM develops and maintains an accreditation/certification support documentation package for system(s) for which they are responsible. Both the SSO and the IAM shall maintain control of any IS, regardless of classification level or sensitivity, introduced into a SCIF so that it is operated, maintained, and disposed of in accordance with internal security policies and procedures as outlined in the accreditation/certification support documentation package.

3. CABLE INSTALLATION. Any area supporting SCI processing shall be accredited by DIA and safeguarded as a SCIF prior to installation. All IT cabling and infrastructure that supports secure communications will be stored in a secured area until used or decommissioned. Cabling and cable connectors shall be color coded to distinguish their classification level. If color coding is not possible, cabling shall be clearly marked to denote their classification level. All cabling shall enter a SCIF from a single location and must be identified and labeled with its purpose and destination at the point of entry. All cabling installations must be installed in accordance with TEMPEST requirements spelled out by a DIA-Certified TEMPEST Technical Authority. All excess old cabling that is no longer needed shall be removed. DIA installation personnel must be U.S. citizens who have been subjected to a favorable NCIC and NAC check. Installation personnel without the proper clearance shall be escorted by cleared personnel. Cleared IT professionals or Construction Surveillance Technicians (CSTs) shall be used to monitor the installation of cabling and infrastructure supporting JWICS networks. The number of escorts and CSTs shall be specified in the Construction Security Plan (CSP).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AIS	automated information system
CAB	compartmented address book
COMSEC	communications security
COR	contracting officer representative
COTR	contracting officer technical representative
CSA	cognizant security authority
CSSO	contractor special security officer
CSP	construction security plan
CST	construction surveillance technician
CTS	courier transfer station
DAC	DIA Deputy Director for Mission Services, Counterintelligence and Security Office
DCID	Director of Central Intelligence Directive
DCD	Defense Courier Division
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoDIIS	DoD Intelligence Information Systems
DoDD	DoD Directive
DoDI	DoD Instruction
DSSCS	Defense Special Security Communication System
DSSS	Defense Special Security System
EAP	emergency action plan
FOUO	for official use only
HCS	HUMINT Control System
HUMINT	human intelligence
IA	information assurance
IAM	information assurance manager
IAO	information assurance officer
IC	intelligence community
ICD	Intelligence Community Directive
IR	infrared
IS	information system
JDS	Joint Dissemination System
JPAS	Joint Personnel Adjudication System

JWICS	Joint Worldwide Intelligence Communication System
LAN	local area network
M-FOM	multi-function office machines
MR	manual review
NdA	nondisclosure agreement
NdS	nondisclosure statement
NGA	National Geospatial-Intelligence Agency
NOFORN	not releasable to foreign nationals
NRO	National Reconnaissance office
NSA/CSS	National Security Agency/Central Security Service
NSI	national security information
NSTISSAM	national security telecommunication and information systems security advisory memorandum
OADR	originating agency's determination required
OCA	office of congressional affairs
PDS	protected distribution system
POC	point of contact
RELIDO	releasable by information disclosure official
RF	radio frequency
SAP	special access program
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SI	special intelligence
SIO	senior intelligence official
SSO	special security officer
SSR	special security representative
STE	secure terminal equipment
STU III	secure telephone unit III
TCO	TALENT Control Officer
TK	TALENT KEYHOLE
T-SCIF	tactical sensitive compartmented information facility
USA	U.S. Army
USAF	U.S. Air Force
USC	U.S. Code
USD(I)	Under Secretary of Defense for Intelligence
USMC	U.S. Marine Corps
USN	U.S. Navy

PART II. DEFINITIONS

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

accreditation. The official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

authentication. Defined in Reference (~~ah~~*ac*).

authorized inspector. A Government or contractor representative of the CSA who is certified and appropriately SCI-indoctrinated for unrestricted access within a DIA-accredited SCIF.

availability. Defined in Reference (~~ah~~*ac*).

CAB. An electronic database register of DoD and U.S. military SSOs. The CAB is a component of the DIA Joint Dissemination System (JDS) that is accessible via JDS links on the INTELINK DIA homepages or directly on INTELINK SCI at https://ismapp3.dia.ic.gov:4444/pls/jds/jds.login1 and on INTELINK SIPRNET at http://206.36.138.26:1776/jds/plsql/jds.login.

certification. Comprehensive evaluation of the technical and non-technical security features and other safeguards, made as part of and in support of the accreditation process, to establish the extent that a particular design and implementation meet a specified set of security requirements.

confidentiality. Defined in Reference (~~ah~~*ac*).

derivative classification. Incorporating, paraphrasing, restating, or generating in a new form information that is already classified.

foreign flag aircraft. An aircraft owned or operated by a foreign government or a non-U.S. carrier.

indoctrination. Formal instruction to an individual approved for access to SCI regarding program-unique information and program-specific security requirements and responsibilities.

inspectable space. The three-dimensional space surrounding equipment that processes classified or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify and remove a potential TEMPEST exploitation exists. Inspectable space may include parking areas around the facility which are owned or randomly inspected daily by the organization, public roads along which parking is not allowed, heavily wooded or other undeveloped areas with restricted vehicular access, and any areas where U.S. security personnel have unannounced 24-hour access.

integrity. Defined in Reference (~~ah~~*ac*).

letter of transmittal. A letter, memorandum, or other correspondence that transmits classified information as enclosures is referred to as a letter of transmittal.

non-accountable SCI. SCI material that does not require document accountability (i.e., document accountability numbers, copy numbers, annual inventory, and certificates of destruction).

non-repudiation. Defined in Reference (~~ah~~*ac*).

SIO. The highest ranking military or civilian individual charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, command, or element of a DoD intelligence organization.

SCI. Defined in Reference (d).

risk management. Management approach that balances the threat and vulnerabilities against the cost of security countermeasures and selects a mix of measures that provide protection without excessive cost in dollars or in the efficient flow of information to those who need it.

working materials. Those materials created during preparation of finished accountable documents and material.