Department of Defense
MANUAL

NUMBER 5105.21, Volume 3
October 19, 2012
Incorporating Change 2, Effective September 14, 2020

USD(I&S)

SUBJECT: Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each serving a specific 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 (DCI) 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 DCI and Director of National Intelligence (DNI) policies for SCI.

b. Volume. This Volume:

(1) Addresses the administration of personnel security for DoD personnel considered for and granted access to SCI.

(2) Provides administrative guidance and procedures for the administration of industrial security, SCI access for the Executive, Legislative and Judicial branches, security incidents, and the security education, training, and awareness program within the DoD.

2. APPLICABILITY. This Volume:

a. Applies to:

(1) 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.b., the DoD Field Activities, and all

other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

(2) Contractors in SCIFs 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.

b. Does not apply to the National Security Agency/Central Security Service, 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. RESPONSIBILITIES. See Enclosure 2 of Volume 1 of this Manual.

4. PROCEDURES. General procedures for SCI administrative security are found in Enclosure 3, Volume 1 of this Manual. Procedures for personnel security, industrial security, SCI access for members the Executive, Legislative, and Judicial branches, SCI security incident reporting, and security education, training and awareness are detailed in Enclosures 2, 3, 4, 5, and 6 respectively of this Volume.

5. RELEASABILITY. **Cleared for public release.** This Volume is available on the Directives Division Website at https://www.esd.whs.mil/DD/.

6. SUMMARY OF CHANGE 2. This administrative change updates the title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security in accordance with Public Law 116-92 (Reference (e)).

7. EFFECTIVE DATE. This Volume is effective October 19, 2012.

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Personnel Security
3. Industrial Security
4. SCI Access for the Executive, Legislative, and Judicial Branches
5. Security Incidents
6. Security Education, Training and Awareness (SETA) Program

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD 5105.21-M-1, "Department of Defense Sensitive Compartmented Information Administrative Security Manual," August, 1998 (cancelled by Volume 1 of this Manual)
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended
(c) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended
(d) Director of Central Intelligence Directive 6/1, "Security Policy for Sensitive Compartmented Information and Security Policy Manual," March 1, 1995[1]
(e) Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019
(f) 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
(g) Section 3001 of title 50, United States Code (also known and subsequently referred to as "Intelligence Reform and Terrorism Prevention Act of 2004"
(h) Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008
(i) Intelligence Community Policy Guidance 704.4, "Reciprocity of Personnel Security Clearance and Access Determinations," October 2, 2008
(j) Intelligence Community Directive 709, "Reciprocity for Intelligence Community Employee Mobility," June 10, 2009[2]
(k) Intelligence Community Policy Guide 704.1, "Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 2, 2008
(l) Intelligence Community Policy Guidance 704.2, "Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 2, 2008
(m) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended
(o) Executive Order 13526, "Classified National Security Information," December 29, 2009
(p) Director of National Intelligence Policy Memorandum 2006-700-8, 'Intelligence Community Modifications to DCID 6/1 Supplement "Security Policy Manual for SCI Control Systems,"' July 12, 2006
(q) Appendix 3 to title 18, United States Code (also known and subsequently referred to as "Classified Information Procedures Act or "CIPA")
(r) Section 783 of title 50, United States Code

[1] Available at http://www.intelink.ic.gov/sites/cps/policystrategy/policy/pages/dcids.aspx [JWICS]
[2] Available at http://www.intelink.ic.gov/sites/cps/policystrategy/policy/pages/dcids.aspx [JWICS]

(s) Intelligence Community Policy Guide 704.3, "Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes," October 2, 2008
(t) DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019
(u) DoD Manual 5220.22, Volume 2, "National Industrial Security Program: Industrial Security Procedures for Government Activities," August 1, 2018
(v) Director of Central Intelligence Directive 7/6, "Community Acquisition Risk Center," March 02, 2005[3]
(w) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," March 18, 2008
(x) Intelligence Community Standard 705-1, "Physical and Technical Security Standards for Sensitive Compartmented Information Facilities," September 17, 2010
(y) Intelligence Community Directive 702, "Technical Surveillance Countermeasures," February 18, 2008
(z) DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
(aa) Intelligence Community Directive 701, "Security Policy Directive for Unauthorized Disclosures of Classified Information," March 14, 2007
(ab) Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008
(ac) Chapter 47 of title 10, United States Code (also known as the Uniform Code of Military Justice)

[3] A Available at http://www.intelink.ic.gov/sites/cps/policystrategy/policy/pages/dcids.aspx [JWICS]

ENCLOSURE 2

PERSONNEL SECURITY

1. GENERAL. The protection of SCI is directly related to the effectiveness of the personnel security program. Intelligence Community Directive (ICD) 704 (Reference (f)) establishes the personnel security standards for the Intelligence Community (IC). An interlocking and mutually supporting series of program elements (e.g., need to know, investigation, binding contractual obligations on those granted access, security education and awareness, individual responsibility, and continuing evaluation) provide reasonable assurances against compromise of SCI by those authorized access to it.

2. APPROVAL AUTHORITY

a. Access eligibility to SCI is granted by a determination authority as delegated by the appropriate Head of an Intelligence Community Element (HICE) having cognizance of the individuals involved. Within the DoD, access eligibility is reciprocal except for interim personnel security clearances. The central adjudication facilities (CAFs) of the following components are authorized to grant, deny, or revoke SCI access eligibility in accordance with Reference (f).

(1) The Department of the Army.

(2) The Department of the Navy.

(3) The Department of the Air Force.

(4) The Defense Intelligence Agency.

(5) The National Security Agency.

(6) The National Geospatial Intelligence Agency.

b. HICEs may delegate authority to the senior intelligence official (SIO) to approve the need to know for Special Intelligence (SI)), TALENT KEYHOLE (TK) GAMMA, and Human Intelligence (HUMINT) Control System (hereafter referred to collectively as SCI) accesses for personnel under their security cognizance, including contractors, consultants, members of the Reserve Component, Government departments or agencies involved in DoD activities , and members of boards and other applicable activities. SIO approval authority shall not be further delegated.

(1) Director, DIA, as a HICE, delegates to the SIOs of the Combatant Commands, the Defense Agencies, and the DoD Field Activities under DIA security cognizance, the authority to approve the need to know for SCI accesses, including special purpose accesses, for personnel

under their respective security cognizance, including contractors, members of the Reserve Component, personnel from non-National Intelligence Board (NIB) member Government departments or agencies involved in DoD activities, and members of boards and other applicable activities.

(2) HICEs and SIOs are responsible for stringent application of SCI security policy and procedures and the need to know principle. They are responsible for ensuring that only those personnel with a validated operational requirement for SCI access are nominated for SCI to preclude unnecessary investigations and adjudications with their attendant cost.

c. The Director of National Intelligence (DNI) (through the Central Intelligence Agency (CIA) Office of Security) grants SCI access for individuals in non-NIB member Government departments or agencies.

d. Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Reference (g)) requires that security clearance background investigations and SCI determinations be accepted by all government departments or agencies, with limited exceptions when necessary for national security purposes. Pursuant to Executive Order 13467 (Reference (h)), the DNI also serves as the Security Executive Agent with certain responsibilities over personnel security processes across the federal government, to include ensuring reciprocal recognition of eligibility for SCI access. In June 2005, the Office of Management and Budget (OMB) assigned the responsibility to arbitrate and resolve case-specific disputes among departments or agencies involving the reciprocity of security clearances and access to SCI to the DNI. Pursuant to Reference (g), DoD Components may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination where appropriate) that exceed security requirements established by executive order without the approval of the DNI and the Director, OMB.

(1) ICD 704 (Reference (f)) requires IC elements and the CAFs to accept all "in scope" personnel security investigations and access determinations that are void of conditions, deviations or waivers. Intelligence Community Policy Guidance (ICPG) 704.4 (Reference (i)) defines "in scope" investigations as those that are less than seven years old. As a matter of DoD policy, all DoD Components shall follow References (f), (i), ICD 709 (Reference (j)), ICPG 704.1 (Reference (k)), and ICPG 704.2 (Reference (l)). Reference (i) also requires that any denial of reciprocity for an eligibility determination that is “in scope” and without exceptions shall be reported to the DNI. DoD Components shall make such reports through the Office of the Under Secretary of Defense for Intelligence and Security.

(2) Reference (k) establishes the personnel security investigative standards and procedures for SCI access. Under reference (k), reinvestigations of personnel eligible for reciprocity are required if their last personnel security investigation was completed more than 5 years ago or if they had a break in service or government employment for more than 24 months. To preserve reciprocity, the reinvestigation must be in progress within 7 years from the completion of previous investigation.

(3) Access eligibility determinations made on the basis of an exception to Reference (l) personnel security standards or investigation standards are subject to review and acceptance by the gaining HICE. The HICE or designee making eligibility determinations based on an exception as specified in paragraph F of Reference (f) shall ensure that the Joint Personnel Adjudication System (JPAS) is updated.

3. ICD 704 ELIGIBILITY. References (k) and (l) mandate personnel security standards for investigation and adjudication eligibility for access to SCI. A single scope background investigation (SSBI) or periodic reinvestigation (PR) that is current or "in scope" will serve as the basis for granting access approval.

a. Only individuals who shall have more than 1 year of job or position tenure after SCI indoctrination should be nominated.

b. Nominees must not have had a break greater than 24 months in Military Service or Federal civilian employment, or in access to classified information pursuant to the National Industrial Security Program (DoD 5220.22-M and Supplement 1 to DoD 5220.22-M (References (m) and (n))).

c. If individuals have a current SSBI or PR but are not SCI-indoctrinated, they must undergo a personal screening interview covering the period since the completion of the last investigation to assure that they continue to meet the standards of Reference (f). The SCI screening interview shall be conducted by the cognizant SSO or designated security official (See Appendix 1 to this enclosure for interview format). If adverse information is disclosed, the appropriate CAF shall be expeditiously notified.

d. In exceptional cases, the HICE or designee may determine that it is in the national interest to authorize temporary access to SCI prior to completion of the required investigation (See paragraph 8.a. of this enclosure). Contractor companies must have a final and current facility clearance (FCL) before contractor personnel can be granted temporary access to SCI. Valid FCLs are reciprocal and facility reviews will not be repeated for multiple contracts IAW DoD 5220.22-M.

e. Requests for investigation shall be submitted to the Office of Personnel Management in accordance with current guidance from the investigation provider. The appropriate CAF shall adjudicate all SSBIs and PRs.

f. JPAS is the DoD personnel security system of record and shall be used to record SCI eligibility determinations and indoctrination authority. SCI indoctrinations in JPAS not accompanied by an owning SCI Security Management Office (SMO) will not be considered valid. SCI SMO ownership indicates continued and valid need to know.

4. REQUIREMENTS FOR SCI ACCESS

a. The HICE or designees may grant SCI access for Federal civilian employees and U.S. military personnel after favorable accomplishment of each of the following:

(1) Pre-nomination interview prior to indoctrination to SCI.

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

(3) Favorable determination of the individual's eligibility as detailed in Reference (f).

(4) Completion of pre-nomination interview prior to SCI indoctrination. Guidelines for pre-nomination interviews are included in Appendix 1 to this Enclosure.

(5) Signing of a Non-Disclosure Statement (NdS) by the individual.

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

b. The HICE or designees may grant SCI access to U.S. contractor employees under the following conditions.

(1) A DD Form 254, "Contract Security Classification Specification," certifies that the contract for which the work shall be performed requires SCI access.

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

(3) The appropriate U.S. Government Contracting Officer's Representative (COR) endorses the requirement.

(4) The requirements in paragraphs 4.a.(3) through 4.a.(6) of this enclosure are successfully completed.

5. THE NEED TO KNOW PRINCIPLE. The primary security principle in safeguarding SCI is access only by those persons with an appropriate clearance, access approval, clearly identified need to know, and appropriate indoctrination. Even when approved for a specific access, the holder is expected to practice need to know in acquiring or disseminating information about the program(s) or project(s) involved.

a. Intrinsic to this discipline is acquiring or disseminating only that information essential to effectively carrying out the assignment. No person shall be deemed to have a need to know solely by virtue of rank, title, or position.

b. When a previously established need to know no longer exists due to reorganization, reassignment, change in duties, or any other reason, the SCI access approval affected by this change shall be cancelled and the individual shall be debriefed.

6. SCI ACCESS MANAGEMENT

a. JPAS shall be the source of individual and collective personnel security data that enables effective SCI access management. The HICEs shall approve individuals for SCI access based on mission requirements and the individual's need to know. The HICE or designee shall manage the granting of SCI accesses in a manner that shall:

(1) Record all SCI indoctrinations and debriefings in JPAS.

(2) Identify the number of accesses granted, denied, revoked, and suspended.

(3) Identify an individual's SCI eligibility date, SSBI date, SSBI-PR date, SCI NdS date, accesses, and exception(s).

b. The HICE shall issue administrative procedures for granting SCI accesses to Government and contractor personnel in accordance with Reference (f).

c. When JPAS is unavailable, the IC's security clearance repository "Scattered Castles" is the alternative system for verifying clearances and SCI accesses.

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

a. NdS. As a condition of access to SCI, individuals must sign a DNI-authorized NdS that includes a provision for prepublication review (DD Form 1847-1, "Sensitive Compartmented Information Nondisclosure Statement"). The NdS establishes explicit obligations on both the Government and the individual for the protection of SCI. An NdS is binding for life and cannot be revoked or waived. Failure to sign an NdS shall result in denial of SCI access.

b. Classification. The NdS is unclassified; however, in certain cases, the fact that a particular person signed an NdS and that the position requires SCI access establishes a relationship that may be classified. The responsible SCI security officer shall ensure that a completed NdS is classified, if required by a program classification guide and record it in the appropriate secure system of record.

c. NdS Completion Procedures. The SCI security officer shall determine if an individual has previously signed an NdS and so verify in JPAS. If verified, no further action is required. If the SCI security officer cannot determine that an individual has signed an NdS, the individual shall sign an NdS prior to receiving access. There is no prohibition against an individual having more than one signed NdS. The security official shall take the following actions in sequence:

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

(2) Provide the individual the opportunity to read the applicable portions of Executive Order (EO) 13526 (Reference (o)) and statutes cited in the NdS. Security officers should use a copy of Standard Form 312 to respond to questions. If questions arise that cannot be answered, the NdS shall not be completed until questions are resolved by the appropriate HICE or designee.

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

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

(b) Supporting SCI security officers shall coordinate with appropriate offices to ensure that personnel are aware that a position may require the completion of the NdS.

(c) The appropriate HICE or designee must be advised as soon as possible if an individual refuses to sign an NdS.

(4) Instruct the individual to complete the form in ink using his or her signature. All appropriate blanks on the NdS form must be completed legibly (printed or typed).

(5) Instruct the witness to sign the NdS in ink using his or her payroll signature. Signing the NdS shall be witnessed and accepted for the Government by a military member or a Federal employee. A contractor may not accept the NdS.

(6) Annotate JPAS with the date that the NdS was signed and the HICE to whom the NdS was sent for retention. Organizations administering the NdS may keep a copy if desired and may provide a copy to the individual at the time of completion.

d. NdS Retention. The cognizant HICE or head of the intelligence and counterintelligence elements of the Military Services is responsible for retaining in a retrievable manner the original NdS for at least 70 years or until death of the individual. This includes contractor NdSs.

e. Indoctrination for Access

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

(a) Special security officers (SSOs) and authorized contractor special security officers (CSSOs) shall use any briefing video approved by the DIA Counterintelligence and Security Office (DAC) as the core indoctrination for access to SI/TK compartments.

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

(c) SSOs shall instruct the individual about prepublication review prior to public release and about outside activities. (See section 15 of this enclosure for additional guidance.)

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

(3) Each time an individual is indoctrinated for SCI access, he or she shall complete a DD Form 1847-1, "Sensitive Compartmented Information Nondisclosure Statement."

(a) The servicing SSO shall use a DAC approved video as the core indoctrination for access to SI/TK compartments.

(b) The servicing SSO shall promptly update JPAS to reflect the control systems for the indoctrinated individual.

f. Post-Indoctrination Change in Status. The local SCI security official or SSO shall conduct the following (and document such actions) in support of a notification of intent to marry or cohabit with a foreign national:

(1) A local agency check on the intended spouse or cohabitant (to the extent possible dependent on the local situation).

(2) A risk assessment that weighs the value afforded the U.S. national security by the individual's continued SCI access eligibility against the risk posed by the intimate relationship with the foreign national.

(3) Completion of appropriate single agency checks via the Office of Personnel Management on the foreign national intended spouse or cohabitant and immediate foreign family members.

(4) Written counseling of the indoctrinated person regarding the automatic reevaluation of their SCI eligibility and the potential adverse effects of this action on their continuing SCI eligibility.

8. SPECIAL CIRCUMSTANCES. Requests for access in special circumstances, including national emergency situations and hostilities, must be based on the urgent need of an organization to prevent failure or serious impairment of missions or operations that are in the best interest of the national security.

a. Temporary/Interim Eligibility for Access to SCI. The HICE or designee may determine that it is in the national interest to authorize temporary access to SCI before completion of the required investigation

(1) The nominating SCI security office shall:

(a) Review the pending SF 86 for a favorable determination.

(b) Make the appropriate local records checks that are immediately possible and conduct a pre-nomination personal security interview of the individual wherever possible and practicable. Local records check should include, at a minimum, a review of criminal records in the jurisdiction where individual lives, review of military police records (if applicable), and local security records. If feasible, a trained security or counterintelligence person should conduct the personal interview.

(c) Document the manner in which the individual's access shall be strictly controlled while the full investigation and a final evaluation are completed.

(d) Transmit requests for temporary or interim eligibility determination to the appropriate DoD CAF using JPAS.

(2) DoD CAFs shall process requests for temporary SCI eligibility in accordance with (Reference (h)).

(3) Temporary eligibility for access to SCI is valid only at the organization granting it and at other agencies that expressly agree to accept it and acknowledge understanding of its investigative basis.

(4) During a national emergency or hostilities, HICEs or their designees may authorize immediate access to SCI for any non-indoctrinated U.S. citizen if the tactical situation and national security require such urgent and immediate access. Such access shall be terminated when the tactical situation allows. As soon as practical, the supporting SSO shall:

(a) Document this decision.

(b) Have the individual execute a nondisclosure agreement (Standard Form 312) or NdS (DD Form 1847-1).

(c) Initiate a request for interim or temporary SCI access.

b. Access by Former Senior DoD Officials. DoD Components may request that retired general or flag officers and Senior Executive Service (SES) civilians participate in DoD-sponsored events when their specific expertise is vital. The HICE may grant access under the condition that the SCI or materials involved are not removed from the confines of a Government installation or other areas approved for SCI. SCI disclosed should not create a conflict of interest for the individuals or give them or their employer (present or potential) a competitive advantage.

(1) A general or flag officer or SES civilian in the DoD Component shall sponsor the request for SCI eligibility and access.

(2) The individual must meet Reference (f) eligibility standards for SCI access.

(3) The request shall provide a justification of need to know.

(4) The requester shall forward all requests to the appropriate HICE or designee no later than 10 working days before access is required. Periods of access shall be valid no longer than 1 year.

c. Access by Retired U.S. Government Employees. Upon retirement or separation from the Federal Government, all collateral clearances and SCI accesses shall be terminated and the individual shall be debriefed. On a case-by-case basis, a retired U.S. Government employee functioning as a non-paid consultant may be granted SCI access not to exceed 1 year under the following conditions:

(1) The individual meets SCI eligibility standards as determined by the sponsoring HICE or designee.

(2) The sponsoring HICE or designee validates the requirement and gives personal approval for SCI access.

d. Special Purpose Access (SPA). Individuals, for example Reserve Component personnel, students, or persons participating in U.S. military exercises, occasionally require access to SCI to perform a specific task. The HICE or designee may grant access not to exceed 180 days.

(1) The SPA shall be approved based on the criticality of the need to know and a favorable Reference (f) eligibility determination from the appropriate CAF as entered in the DoD personnel security clearance system of record.

(2) Upon approval, the individual shall be given an indoctrination briefing which includes the basic information to protect SCI. The individual shall sign an NdS and be indoctrinated for the appropriate SCI access.

(3) Records of indoctrination for SPA shall include specific date of automatic debrief from SCI access. Extensions must be requested and approved before the automatic debrief date.

e. Details and Temporary Duty

(1) When an individual from the DoD is detailed to a position in the Executive Office of the President or a board or activity not under the security cognizance of the Department, the authority determining the need to know is responsible for briefing and debriefing the individual and shall obtain concurrence from the parent DoD Component prior to granting access.

(2) The indoctrination of individuals on temporary duty assignment requiring access to SCI is primarily the responsibility of the parent department or agency. However, the parent department or agency may ask the temporary duty station to provide indoctrination assistance. Whenever practicable, indoctrination assistance requests should be processed via JPAS.

(3) DoD Components providing indoctrination assistance should input the indoctrination data in the individual's JPAS record and forward the SCI indoctrination paperwork to the individual's home-station SSO.

f. Military Reserve Personnel and National Guard. The Military Services are responsible for certifying SCI access eligibility of their assigned reservists and National Guard personnel (Army and Air Force). The SSBI and SCI access eligibility for reserve and National Guard personnel are acceptable if the investigation is current or "in scope" and an SCI screening interview indicates no major change in personal status that would affect their access eligibility. Reserve and National Guard personnel who no longer meet these requirements must be processed in accordance with this enclosure. Reserve and National Guard personnel may be immediately re-indoctrinated for SCI access upon arrival under the following conditions:

(1) They possess a current SSBI or PR.

(2) They are currently assigned in either a direct support unit manning position, an individual mobilization augmentee (IMA), or a mobilization designee (MOBDES) position on a recurring basis to the command.

(3) They are currently SCI eligible authorized by the appropriate Service CAF.

(4) Reservists shall be afforded access only to the level of SCI required to successfully perform the reserve tour as defined by the SPA justification. They shall not be granted SCI access for convenience.

(5) Reservists who require SCI access for their 2-week duty tours, but whose weekend duties do not require SCI access, should be provided an SPA for the 2-week tour. SCI access authorized to reservists in connection with their reserve duties may not be used in connection with civilian or contractor employment.

(6) The appropriate joint agency shall indoctrinate and debrief reservists assigned to joint service positions.

(7) Reservists and National Guardsmen assigned to IMA or to MOBDES positions and who require SCI access shall be determined SCI eligible, indoctrinated to required accesses, and debriefed at termination of assignment.

(8) Reservists who are also SCI-indoctrinated contractors shall receive a conflict of interest education briefing as part of their initial indoctrination by the local SCI security official and shall sign a conflict of interest acknowledgment. (See Appendix 2 to this enclosure for the briefing.)

g. Contractor Access. U.S. contractors and supporting U.S. Government SSOs may request and use DoD employee certifications held by another DoD agency or department, provided that the U.S. Government contractor's SCI need to know has been established and approved by the appropriate HICE.

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

i. Proximity Access. Proximity access is no longer authorized in accordance with DNI ICPM 2006-700-8 (Reference (p)).

j. Intergovernmental Personnel Act (IPA) Access. IPA employees are individuals who are detailed or appointed to temporary positions within the Federal Government. Individuals are sometimes recruited from outside the Federal Government and designated as IPAs on temporary assignments in order to gain benefit of their unique, special skills. Procedures and requirements for SCI eligibility and indoctrination of Federal Government employees described in this Volume apply to IPAs. IPAs shall be processed as civilians and meet all investigative and adjudicative requirements prior to being provided SCI access.

9. SUSPENSION OR REVOCATION OF SCI ACCESS. When the need to know for SCI has ceased or an individual’s access to SCI is suspended or revoked, the individual shall be denied further access to SCI. The SSO (or CSSO, if appropriate) is responsible for accomplishing and reporting the debrief action in JPAS and for canceling all current visitor certifications pertaining to the debriefed individual. Upon notification from the Cognizant Security Authority (CSA) that an individual’s SCI accesses have been suspended or revoked, the SSO or CSSO shall immediately cancel all certifications and notify the CSA that such action was completed.

a. Debriefings. As a minimum, debriefings shall include:

(1) Reading the appropriate sections of the appendix to title 18, United States Code (U.S.C.) (Reference (q), hereafter referred to as the “Classified Information Procedures Act” or “CIPA”) and section 783 of title 50, U.S.C. (Reference (r)), thereby reminding the individual of the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure.

(2) Reading a statement emphasizing the requirement for continued protection of SCI and the responsibilities incurred by the NdS. Acknowledgment of the continuing obligation of

the individual under the prepublication and other provisions of the NdS never to divulge, publish, or reveal by writing, spoken word, conduct or otherwise, to any unauthorized persons any SCI without the written consent of appropriate department or agency officials.

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

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

(5) Signing a DD Form 1848, "Sensitive Compartmented Information Debriefing Memorandum." The DD Form 1848 is unclassified when using the DNI approved digraphs or trigraphs.

(6) Updating the clearance system of record with the debrief status by the cognizant SSO.

b. Suspension of SCI Access. DoD HICEs shall maintain active programs to monitor the continued security eligibility of SCI-cleared personnel. SSOs should maintain effective liaison with supervisory personnel, to identify as early as possible potential security problems involving SCI-indoctrinated personnel.

(1) When information of obvious security concern develops:

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

(b) The SCI security officer shall expeditiously remove SCI access from JPAS and work with the commander or official to determine how the issue may affect the individual's continued eligibility for SCI under the OMB Adjudicative Guidelines contained in Reference (i) and whether the issue requires action by the cognizant CAF. (See Figure 1 for format.)

(2) Local SCI access suspension is a temporary measure designed to safeguard sensitive classified information or facilities while the issue of concern is investigated. If the commander or official decides the issue warrants reporting to the cognizant CAF, the SCI security officer will use JPAS.

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

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

(c) Once submitted, only the cognizant CAF can make a final determination regarding the individual's continued SCI eligibility. Figure 1 provides a template for suspension report to be provided to CAFs.

(3) Individuals who have had their SCI access suspended, or have received a final denial or revocation of security clearance, may not enter a SCIF except with HICE or designee approval.

Figure 1. SCI Access Suspension Report Format

SUBJ: SUSPENSION OF SCI ACCESSES

1. NAME, RANK, SERVICE, SOCIAL SECURITY ACCOUNT NUMBER (SSAN)

2. STATEMENT THAT THE COMMANDER (SPECIFY UNIT/BASE) HAS SUSPENDED SCI ACCESS.

3. REASON FOR SUSPENSION:

4. STATEMENT WHETHER AN INVESTIGATION HAS BEEN REQUESTED AND, IF SO, WHEN AND BY WHOM.

5. STATEMENT OF ACTION TAKEN.

6. TYPE OF PERSONNEL SECURITY INVESTIGATION AND AGENCY THAT CONDUCTED THE INVESTIGATION.

7. ORGANIZATION TO WHICH ASSIGNED.

8. SCI ACCESSES HELD, IF INDOCTRINATION PENDING, SO STATE.

9. ANY PUBLICITY ANTICIPATED AND TO WHAT EXTENT

c. Incident Reports. When an individual is debriefed from all SCI access for cause, the SSO shall submit an Incident Report via JPAS to the supporting CAF. The report shall specify reason for report, accesses held, indoctrination and debriefing dates, a justification for the debriefing, and any other pertinent information (see Figure 2). Individuals debriefed for cause shall only be re-indoctrinated following favorable adjudication by the cognizant CAF.

Figure 2. Incident Report Format

FM: LOCAL SSO

TO: (SUPPORTING ADJUDICATION FACILITY)

INFO: SSO (AS REQUIRED)

CLASSIFICATION (AS REQUIRED)

SUBJ: DEROGATORY REPORT

1. LAST NAME/FIRST NAME/MIDDLE INITIAL/SURNAME., ETC.

2. RANK/SERVICE/SSN DESIGNATOR OR MOS.

3. ACCESSES AND DATES DEBRIEFED.

4. REASON FOR REPORT.

5. CERTIFICATION OF SCI ELIGIBILITY/REFERENCE/SSBI DATE/CCN

6. SCI NdS DATE/FINAL TOP SECRET DATE.

7. REMARKS (AS REQUIRED).

d. Appeals Process. All personnel who are the subject of an adverse SCI eligibility determination are afforded the opportunity to appeal the determination subject to the provisions of ICPG 704.3 (Reference (s)). The determination authority is responsible for providing appeal procedures. The following requirements apply equally to denials or revocations of SCI access. Individuals shall be:

(1) Provided a comprehensive and detailed written explanation of the reasons for the intended denial or revocation.

(2) Provided upon request, to the extent permitted by law, any documentation upon which a denial or revocation was based.

(3) Informed of the right to be represented by counsel or other representative at their own expense and of their right to request documents.

(4) Provided an opportunity to reply in writing within 45 days of receipt of relevant documentation and to submit evidence on his or her behalf.

(5) Provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal.

(6) Provided an opportunity to appeal in writing to a higher level Appeals panel.

(7) Provided an opportunity to appear personally and present relevant evidence and information before an adjudicative authority or other authority as determined by the DoD Component head.

e. Reinstatement of SCI Access. Reinstatement of SCI access may be granted under the following circumstances:

(1) Revalidation of need to know by responsible HICE or designee.

(2) Receipt of new favorable SCI eligibility determination by cognizant CAF.

10. RECIPROCITY OF ACCESSES (TRANSFER-IN-STATUS). Individuals who temporarily or permanently transfer to another DoD agency that requires the individual to maintain access to SCI may have their SCI indoctrination paperwork passed from the losing organization to the gaining organization. This transfer eliminates the necessity for the transferring individual to duplicate the indoctrination paperwork at the gaining organization. A transfer-in-status may be initiated by either the losing or the gaining organization's SSO.

11. PERIODIC REINVESTIGATION (PR) PROCEDURES. PRs shall be conducted as prescribed in Reference (k).

a. The PR must be initiated no later than 5 years after the completion date of the last investigation. The individuals concerned shall be contacted to complete a new Standard Form (SF) 86, "Questionnaire for National Security Positions," to cover the period since the last SSBI or SSBI-PR was completed. Fingerprint cards will be submitted through the investigative agency to the Federal Bureau of Investigation for initial investigations.

b. The local SCI security official shall review completed statements of personal history to determine if any relevant personnel security information has been excluded prior to submission to the investigative provider. If the individual fails to submit the requested PR package, SCI security officials should determine the cause (e.g., notification of expiration not received, access no longer required) prior to any automatic termination of SCI access.

12. CHANGES IN PERSONAL STATUS. Individuals with SCI access shall expeditiously notify their respective local SCI security official or CSSO of any significant change in personal

status. Failure to comply with reporting requirements may adversely affect an individual's continuing eligibility for SCI access. Significant changes include but are not limited to the following:

a. Change in Marital Status. Changes in marital status include marriage, intent to marry, or marriage to a foreign national, divorce, or proposed name change. Cohabitants are treated as spouses in this context. Waivers shall be reviewed by the supporting CAF on a case-by-case basis. Marriage to, or cohabitation with, a foreign national shall be grounds for re-evaluation of SCI access. SCI-indoctrinated personnel shall report to the supporting SCI security official or SSO in advance of their intention to marry or live with a foreign national. The notification of marriage or cohabitation shall include:

(1) Complete information of the prospective spouse/cohabitant and his or her immediate family members.

(2) The type of visa or alien status of the intended spouse or cohabitant and their immediate family members (if resident in the United States, its territories, or possessions), and whether these persons intend to become American citizens.

(3) The nature and extent of relationship with the intended spouse or cohabitant's family.

(4) The vocational or political ties of the intended spouse or cohabitant and their immediate family with their government.

b. Change in Association with Foreign Nationals. Casual contact is unplanned, non-recurring contact with a foreign national with no deliberate effort by either party to affect recurrence. Changes in previously reported casual contact with foreign nationals must be reported when such contact develops into close and continuous personal associations.

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

13. EMPLOYEE OUTSIDE ACTIVITIES

a. Potential conflicts with an individual's responsibility to protect SCI material may arise from outside employment or other outside activity to include contact or association with foreign nationals. In cases where such employment or association has resulted in a suspected or established compromise of SCI, the local SCI security official and supporting CI activity must be advised immediately. Involvement in non-U.S. Government employment or activities that raise potential conflicts with an individual's responsibility to protect SCI information is of security concern and must be reviewed by an SCI security official to determine whether the conflict is of such a nature that the individual's SCI access should be reevaluated.

b. Individuals who have or are being considered for SCI access must report in writing to the local SCI security official any existing or contemplated outside employment or activity that meets the two criteria below. In addition, an initial or updated SF 86 must include details of such outside employment or activities.

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

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

c. The provisions of this section of this enclosure (paragraphs 13.a. and 13.b., in their entirety) shall be made available to individuals for reading during SCI indoctrination. Annual security education for SCI-indoctrinated individuals shall advise them:

(1) To report in writing to their local SCI security officer any existing or contemplated outside employment or activity that appears to meet the above criteria.

(2) That the written report must be submitted before accepting the outside employment or activity.

14. PERSONNEL SECURITY FILES. SSOs shall maintain the following information:

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

(1) SCI indoctrination information, SCI debriefing, and a copy of DD Form 1847-1; unless JPAS shows the date the NdS was previously executed. (CSSOs shall maintain copies of this information as provided by the CSA or supporting SSO, or as produced in fulfilling their responsibilities as CSSO.)

(2) Copies of other pertinent security personnel actions or defensive security briefings and debrief memoranda such as conflict of interest briefings for reservists.

(3) Copies of reports of credible derogatory information, reports of changes in personal status, and other related paperwork such as security violation reports that may adversely affect a

person's continuing eligibility for SCI access or result in referrals to counterintelligence (CI) agencies.

(4) Pre-indoctrination screening interviews, foreign contact reports, foreign travel notifications, foreign travel reports, and the annual briefing on reporting foreign contacts.

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

15. SECURITY PRE-PUBLICATION REVIEW PROCESS

a. Review of Proposed Public Statements. DoD SCI-indoctrinated personnel are encouraged to participate as speakers in recognized forums and to submit professional papers. Such participation encourages the exchange of information and promotes professional growth. All proposed public statements on information derived from SCI or concerning SCI operations, sources, or methods must be reviewed and approved before release by the appropriate HICE or designee.

(1) An SCI-indoctrinated or debriefed individual shall submit for security review, prior to public disclosure in any form, all material intended for disclosure that may contain SCI or SCI-derived information. The material shall be submitted to the department or agency that last authorized the individual's access to such information. Review action must start without delay.

(2) The SCI prepublication review in no way absolves an individual from following the requirements of DoDI 5230.09 (Reference (t)) or other regulations requiring certain military or DoD persons to submit material for review prior to public release.

(3) The SCI security officer receiving the material shall make an initial review and coordinate the review as required. If a determination cannot be made initially as to whether SCI is involved, the material shall be forwarded through SCI channels to the command, Defense Agency, or Military Service level for review.

b. Review of Resumes and Applications for Employment. Resumes or applications for employment which detail technical expertise gained through government employment in classified or sensitive programs must be written in an unclassified context even if the potential employer is known to be a cleared defense contractor. A security review should be requested to resolve questions or concerns regarding possible classified content prior to submission to a potential employer. The following statement is appropriate for use in resumes or applications regarding clearance status when seeking employment with an organization involved in classified programs: "CLEARED FOR TOP SECRET INFORMATION AND GRANTED ACCESS TO SENSITIVE COMPARTMENTED INFORMATION BASED ON SINGLE SCOPE BACKGROUND INVESTIGATION COMPLETED ON (DATE)."

(1) The individual's servicing SCI security official can provide SSBI completion dates and case control numbers. Do not indicate or provide digraphs or trigraphs on a resume or job application.

(2) The local SCI security official shall establish local written procedures for security reviews or pre-publication reviews. The requirements for security review and prepublication review shall be part of the annual security education program. The local SCI security official shall effect proper local coordination with the appropriate Government agency public affairs or information office and conduct a prepublication review for any public release of information that may possibly contain SCI.

16. CONTACT WITH FOREIGN NATIONALS. SCI-indoctrinated personnel must protect themselves against cultivation and possible exploitation by foreign nationals who are or may be working for foreign intelligence services and to whom they might unwittingly provide sensitive or classified national security information. SIOs shall provide implementing guidance for the administration of the following policy, as established in Reference (f), for individuals under their security cognizance.

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

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

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

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

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

c. Defense Attaché System personnel and other personnel whose duties require regular official contact with foreign government representatives and other foreign nationals are exempt from the approval requirements and from reporting of foreign contacts directly associated with their duties, except as required by their agency's regulations. The HICE, designee, or SIO may exempt other personnel, on a case-by-case basis, whose duties require regular contact with foreign nationals.

(1) Defense Attaché System personnel and other personnel whose duties require regular contact with foreign government representatives and other foreign nationals are not exempt from the 72-hour reporting requirement whenever an incident occurs as described in paragraph 16.a. of this enclosure.

(2) Based on the foreign contact report, the SSO or SCI security official may require the reporting individual to complete a foreign contact questionnaire (see Appendix 3 to this enclosure). The SCI security official shall forward a copy to the local supporting CI activity for action and retain an information copy in the individual's personnel security file. Discussions of any contact reports shall be restricted to those with a demonstrated need to know. Under no circumstances shall the individuals involved, their supervisor, or the local SCI security officer make any attempt to investigate such matters. Investigations of any contact reports shall be the responsibility of the appropriate CI activity.

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

e. Local SCI security officers shall ensure that DoD SCI-indoctrinated personnel are briefed annually on their responsibility to report foreign contacts and maintain a record showing the dates that the individuals were briefed.

f. These procedures are not intended to inhibit or discourage contact with foreign nationals. They are meant to properly document and disseminate the contacts and associations and all relevant information obtained.

17. FOREIGN TRAVEL

a. Procedures. Personnel with SCI access who plan official or unofficial foreign travel shall:

(1) Report anticipated foreign travel through their immediate supervisors and to the SSO or local SCI security official (see Appendix 4 to this enclosure). Failure to report foreign travel may result in reevaluation of eligibility for continued SCI access.

(2) Obtain a defensive travel security briefing or a risk-of-capture briefing from your supporting security office prior to travel. Briefings provide situational concepts of threats that can be encountered, regardless of the country of intended travel. Threat situations shall include those from foreign intelligence services, terrorist or narcotics groups, or indigenous groups active in promoting insurgency, war, civil disturbance, or other acts of aggression when physical safety and security of personnel cannot be reasonably provided.

(3) Report any unusual incidents occurring during travel.

b. Defensive Travel Security and Risk-of Capture Briefings

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

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

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

c. Classification Guidance. Details about a traveler's access to SCI or his or her itinerary may require classification as determined by an original classification authority or a security classification guide.

Appendixes

1. Guidelines for the Conduct of Personnel Screening Interviews and Questionnaire
2. Conflict of Interest Security Education Briefing for Reservists
3. Foreign Contact Questionnaire
4. Foreign Travel Questionnaire
5. Defensive Security Briefing

APPENDIX 1 TO ENCLOSURE 2

GUIDELINES FOR THE CONDUCT OF PERSONNEL SCREENING INTERVIEWS AND QUESTIONNAIRES

1. PREPARATION. Before conducting the pre-SCI indoctrination interview, the SSO or SCI security official shall review all available command personnel and security records.

2. SCOPE. Questions asked during the course of an interview must have a relevance to a SCI indoctrination determination. Care must be taken not to inject improper matters into the security interview. For example, religious convictions, opinions regarding racial matters, political beliefs, and affiliations of a non-subversive nature such as membership in labor unions are generally irrelevant topics. The interviewer must be able to explain the relevance of all inquiries, if subsequently required to do so. The screening questionnaire should cover, at a minimum, the questions included in Figure 1 of this Appendix.

3. PROCEDURES

a. The subject should be advised that: the purpose of the security interview is to assist in determining the subject's continued acceptability for access to SCI based upon Reference (f) criteria; the interviewer is not associated with any investigative or law enforcement agency; the subject is not suspected of any wrong doing; the interview is completely voluntary and may be terminated at any time. The subject shall be given the same Privacy Act advisement as was provided with the SF 86. The interview is an administrative screening process; therefore, a warning to the subject about self-incrimination shall not be required.

b. The interviewer shall offer the subject the opportunity to contribute any information the subject feels may be pertinent. The subject shall be informed that the procedure is designed to preclude any future judgment that the subject intentionally withheld significant security issue information.

c. If the subject refuses to be interviewed or declines to provide information in response to specific pertinent questions, contact the appropriate HICE or designee for guidance.

d. The interviewing SSO or SCI security official shall determine whether to continue an individual's SCI access based on the results of the interview or to refer the results to the appropriate CAF for review.

Figure 3. Personnel Screening Interview Question Set

PERSONNEL SCREENING INTERVIEW QUESTIONNAIRE

The purpose of this interview is to assure that you continue to meet the standards for access to SCI in accordance with Intelligence Community Directive 704.

1. Has your marital status changed since you completed your SF 86; have you married or divorced, or begun cohabitating?

2. Are all members of your immediate family U.S. citizens?

3. Do you or anyone in your immediate family claim a dual citizenship with another country?

4. Have you visited any foreign countries since you completed your SF 86? If so, please provide the dates, the countries visited and the reason for the visits.

5. Have you consulted with a mental health professional since you completed your SF 86? Was this court ordered or based on violence on member's part? If yes, please explain.

6. Have you been arrested since your last investigation? If yes, please explain.

7. Have you ever had any adverse involvement with alcohol (e.g., DUI, alcohol treatment, drunk in public, accident where alcohol was a factor)? If so, please explain.

8. Have you used illegal drugs or illicit substances since you completed your last SF 86? If yes, please explain.

9. Have you had a clearance suspended, denied, or revoked since your last investigation or in the last seven years? If yes, please explain.

10. Have you had any bills referred to a collection agency since you last completed an SF 86? If yes, please explain.

11. Have your wages been garnished, have you had any vehicles repossessed, have any tax liens been placed against you, or have you filed bankruptcy? If so, please explain.

APPENDIX 2 TO ENCLOSURE 2

CONFLICT OF INTEREST SECURITY EDUCATION BRIEFING FOR RESERVISTS

Figure 4 Conflict of Interest Security Education Briefing for Reservists Sample

CONFLICT OF INTEREST SECURITY EDUCATION BRIEFING FOR RESERVISTS

1. All personnel granted access to Sensitive Compartmented Information (SCI) are legally bound to protect and safeguard the information under the guidelines set forth by the Nondisclosure Statement (NdS).

2. Reserve military members are authorized to use their SCI access only when they are under official military orders and a valid "need to know" exists. All information protected through the various SCI programs can be used only to support and assist the operational endeavors of the Department of Defense, not the individual or the civilian firm. All personnel must be aware of this delicate balance. Any disregard of these procedures could potentially cause serious security problems to arise or undue embarrassment to the Department. The individual is legally bound by the obligation set forth in the NdS.

3. A few simple precautionary measures can prevent a conflict of interest. The SCI security badge is to be used only when on official military orders. The SCI security badge should be maintained by the administrative office that supports each individual's reserve duties. If there are problems identifying the support personnel, each individual must contact the SSO. Next, verify through the SSO the proper level of SCI accesses. SCI accesses obtained through civilian employment or external Government agencies shall not suffice. All DoD SCI accesses must be authorized and approved through the proper cognizant authority.

4. In summary, any information gained while in an indoctrinated status can be used only in support of military issues. The transfer of SCI from one agency to another, either verbally or by documentation, can only be accomplished through proper security channels. If ever in doubt as to the proper security procedures, contact your local Special Security Office for advice.

APPENDIX 3 TO ENCLOSURE 2

FOREIGN CONTACT QUESTIONNAIRE

1. Foreign contact questionnaires shall contain, at a minimum:

a. Information regarding the foreign contact, such as:

(1) Contact's name, citizenship, and profession/affiliation

(2) Date and place of occurrence of contact.

b. Contact details, such as:

(1) Manner in which the individual initiated contact (e.g. casual contact at foreign function).

(2) Sex and ethnicity of the individual.

(3) Did the individual seem to control the direction of the conversation?

(4) Did the individual ask where you work or what kind of work you do?

(5) Did you discuss your involvement in government-related activities?

(6) Did the individual ask about your political affiliations?

(7) Did the individual offer to pay for anything or make any special arrangement on your behalf?

(8) Have you received any gifts from the individual?

(9) Did you exchange contact information with the individual?

(10) Did the individual express interest in any further contact?

c. A physical description of the individual.

d. A list of topics in which the individual expressed an interest which you believe are classified, sensitive, or proprietary.

2. Once filled out, the contact questionnaire shall be retained by the cognizant security official for additional action as necessary.

APPENDIX 4 TO ENCLOSURE 2

FOREIGN TRAVEL QUESTIONNAIRE

1. Prior to proceeding on either official or unofficial travel outside of the United States, travelers shall complete a foreign travel questionnaire to be returned to the cognizant security official as soon as possible prior to the proceed date. This questionnaire shall elicit, at a minimum:

a. The name, date of birth, place of birth, and SSAN of the traveler.

b. The traveler's job title.

c. The full itinerary for the trip, including flight numbers and arrival/departure times.

d. The purpose of the travel (i.e., business or recreation). If travel is related to official government business, traveler should list the point of contact he/she is to meet with and the purpose of the meeting.

e. The country (or countries) to be visited and the dates of travel.

f. The passport type (i.e., tourist, official, diplomatic), the passport number, and expiration date.

2. Upon return from travel, the traveler shall complete a secondary questionnaire that shall elicit, at a minimum:

a. Were any problems encountered at the time of arrival or departure from the foreign country (or countries)?

b. Was the traveler subjected to any harassment, suspected surveillance, unusual customs inspection, etc., during the trip?

c. Were any travel restrictions imposed by the country (or countries) during the visit?

d. Were any changes made to the itinerary while on route?

e. Were any probing inquiries made relative to the traveler's job duties, studies, or organization (if yes, traveler must complete a foreign contact questionnaire as described in Appendix 10 to Enclosure 2 of this Volume)?

f. Did traveler meet a foreign national who requested future contact (if yes, traveler must complete a foreign contact questionnaire as described in Appendix 3 to Enclosure 2 of this Volume)?

g. Was the traveler a victim of a criminal act?

h. Was the traveler detained or arrested?

i. Did the traveler lose any official materials or personal luggage?

APPENDIX 5 TO ENCLOSURE 2

DEFENSIVE SECURITY BRIEFING

1. INTRODUCTION. Persons granted access to SCI incur special security obligations and should be aware of possible risks inherent to foreign travel. Persons planning foreign travel should contact their SSO to determine their organization's foreign travel and foreign contact policy. The following information is a general purpose travel briefing. Detailed briefings may be obtained from the nearest military intelligence or counterintelligence representative.

2. PURPOSE. U.S. military, Government, civilian and defense contractor personnel are considered prime targets of Foreign Intelligence Services and terrorist groups. The purpose of this briefing is to acquaint the traveler with the risks involved in traveling to foreign countries and to furnish you guidance that may enable you to minimize those risks.

3. BACKGROUND. Many foreign countries offer interesting travel brochures, special rates, and other inducements through U.S. branches of their travel bureaus in efforts to attract the growing number of Americans traveling abroad. Past cases reveal that American personnel performing such travel may be subject to surveillance and collection operations by the various foreign intelligence services. Travelers may also be subject to terrorism or other acts of violence either by design or by circumstance.

4. FOREIGN INTELLIGENCE SERVICES (FIS)

a. All foreign countries actively engage in the collection of intelligence information. However, whether they are "hostile," "neutral," or "allied," there is no such thing as a "friendly" foreign intelligence service.

b. The main objective of any FIS is to gain advantage for their nation through the collection of information. Currently, the most prized type of intelligence is scientific and technological data, followed by the classified Government information, but unclassified material--even material which appears to be trivial can also be of inestimable value. Potentially, the most valuable sources of information are those acquired through the use of individuals recruited as agents by FIS. In addition to penetrating the Government and its official organizations, the penetration of commercial businesses, educational and private institutions involved in sensitive, national defense-related research and development work can be of tremendous value. Of course, the single greatest achievement an intelligence organization can have is the placement or recruitment of an agent directly in a sensitive position in a national defense or intelligence element of another government.

(1) FIS are relentless and seek information wherever, whenever, and from whomever they can and employ any and all tactics necessary to target, recruit and exploit potential sources. Among the tactics they may use against U.S. personnel is a smooth, subtle, seemingly guileless

approach—befriending targets, treating them to gifts or money, wining and dining them in the belief that Americans are hopeless materialists who can be swayed easily by appeals to their greed.

(2) Recognizing that most Americans are generally friendly and gregarious people who enjoy talking to others, FIS operatives frequently employ a seemingly innocuous and very effective method of intelligence gathering known as "elicitation." Elicitation is the art and science of engaging someone in simple, "innocent" conversation for the purpose of getting the targeted individual to speak openly and more in-depth and, possibly reveal classified information on topics of interest to FIS operatives. Practiced by experts, the target of elicitation may not even realize that he or she has been elicited until "too much" has been said. Elicitation is smooth and insidious. Beware of it!

(3) In another maneuver known as the "False Flag" approach, an FIS operative misrepresents himself as a citizen of a country friendly to the United States. Thus, a targeted American may be duped into handing over information by being led to believe he is aiding an ally of the United States. In a variation of this tactic, FIS agents may pose as representatives of a country towards which a targeted American is particularly sympathetic. Also, if an FIS agent believes an individual has similar sympathies, he or she may make an appeal for information based on ideology. A "pitch" for information may also be geared to take advantage of an American's desire for international harmony and world peace. Similarly, certain FIS organizations not only routinely charge their own citizen-students studying abroad in the U.S. to collect information but, also regularly target Americans of their own ethnicity using a variety of tactics to include everything from bribery and patriotic appeals to support their "mother country" to outright blackmail and threats.

(4) Another favored appeal exploits the American belief in freedom of speech and the free exchange of information. For example, an FIS agent in the role of a scientist may suggest to an American scientist that science has no political boundaries. Therefore, in the interest of science, the American is encouraged to share his knowledge with a fellow "member" of the international scientific community.

(5) FIS also use aggressive means in their ceaseless quest for strategic information. Espionage is their business and patriotic duty. If they feel coercion and blackmail shall serve their purpose, they shall not hesitate to employ those methods. As you travel, do not place yourself in a compromising position by engaging in abnormal or promiscuous sexual behavior, black marketing, violating local laws, or photographing or straying into restricted areas. FIS keep travelers under constant surveillance by using agents, video and photographic surveillance, and bugging devices in hotel rooms, bars, restaurants, lounges, and telephones. Such methods may provide them the material to entrap an unwary traveler.

(6) Harassment and provocation are other tools that may be employed by FIS. Travelers may be placed in unusual situations that may cause an incident or elicit a response that would entangle or compromise an individual.

5. TERRORIST, CRIMINAL, AND MOB VIOLENCE

a. Terrorists have a different objective than FIS—they are interested in "sensationalism" or other use that can be derived from the compromise, embarrassment, interrogation, kidnapping, or death of a U.S. citizen. The threat changes constantly and is contingent upon the country and area visited along with world events. However, from a general perspective, the threat of terrorism to a traveler should be considered minimal, unless the traveler happens to be in the wrong place at the wrong time. As with FIS, a terrorist group must know the "who, where, when, and how," to target a specific individual. Therefore, maintaining a "low profile" and not drawing undue attention to one's affiliation with the U.S. Government is essential. Even though an individual may not be targeted for terrorism, an individual can still become a victim of terrorism. Being in the wrong place at the wrong time may be unavoidable, but the risk of being a chance victim of terrorism can still be reduced. Remember, most terrorists select "soft" targets like commercial establishments and individuals residing within that country. For the most part, except in situations where FIS is supporting, sponsoring, or otherwise has a relationship with a particular terrorist organization, terrorists do not have sophisticated collection capabilities to determine names of a traveler and then target that person. They prefer to concentrate on individuals residing in-country.

b. Criminal or Mob Violence. No matter where anyone travels, criminal elements (thieves, muggers, etc.) are present. The foreign traveler is a good target because the traveler may be disadvantaged by being in an unfamiliar place, ignorant of local laws, and unable to freely communicate because of a language barrier. In unstable political areas or where the United States is unwelcome, the presence of a U.S. citizen may be enough provocation to cause an incident or become a victim of mob violence. Any minor incident or breach of law or custom involving a U.S. citizen can be blown vastly out of proportion creating a much larger incident.

6. TRAVEL GUIDANCE. Common-sense rules for any traveler are often overlooked in the rush to acquire tickets, hotel reservations, visas, etc.:

a. Personal Concerns

(1) Travelers should not reference their intelligence affiliation or access to classified information.

(2) Travelers should not bring any personal objects with them that they cannot afford to lose. This applies especially to jewelry items. Carry traveler's checks and one or two major credit cards, not large amounts of cash.

(3) Travelers should make a copy of the identification page of their passport before their departure and take it with them. Copies should be kept separate from the passport itself. Also, travelers should memorize their passport number. While traveling, travelers should leave their passport and any unneeded money locked in a hotel safe-deposit box. If local law does not require persons to keep their passport with them, travelers should carry only the photocopy of their passport and driver's license when leaving the hotel.

(4) Travelers should advise the U.S. Embassy in each host country of their complete itinerary. Keep in contact and record the address and telephone number of the U.S. Embassy or Consulate in each host or major city in which a visit is planned.

(5) Travel with several passport size photos. In some areas, it can be difficult to replace photos on short notice if your passport is lost or stolen.

(6) U. S. driver's licenses are valid in Canada and Western Europe; elsewhere you shall need an international driver's permit available from the American Automobile Association. Even with an international permit, foreigners are forbidden to drive in countries such as Egypt, Vietnam, China, and Nepal. Know local traffic laws and penalties, which may be severe. In Indonesia, for example, fines for not wearing a seat belt can be $1,500.

(7) The Department of State, Bureau of Consular Affairs, Office of Overseas Citizen Services provides current, country-specific threat information and offers consular information sheets, travel warnings, public announcements, tips for travelers brochures, visa bulletins, and other consular information. Callers outside the Washington, D.C. metropolitan area are charged the cost of a long distance phone call, but there are no additional charges for this service. They may also be contacted through the internet at www.travel.state.gov.

(8) Information on vaccinations and other health precautions, such as safe food and water precautions and insect bite protection, may be obtained from the Centers for Disease Control and Prevention's (CDC) hotline for international travelers at 1-877-FYI-TRIP (1-877-394-8747) or via www.cdc.gov/travel for reports of medical alerts in foreign countries.

(9) Travelers should ensure their medical insurance covers the travel. Personal health insurance policies may be valid while you are visiting Europe, but may not cover individuals while white-water rafting in Canada.

(10) Carry ample supplies of pain relievers, antacids, diarrhea and motion-sickness remedies, antibiotic cream, gauze bandages, water-purification tablets, insect repellent, sunscreen and prescription medication.

(11) Travelers should carry prescription medications in their original containers. Travelers can be detained during a custom's search and questioned concerning the pills.

(12) Medical or dental service should be obtained only from a U.S. Government facility or from persons or institutions approved by U.S. Embassy officials.

b. Hotel Concerns

(1) Be careful about leaving items in hotel room safes. Safe-deposit boxes in a hotel lobby are better, but the best are similar to those in a U.S. bank, with two keys and under 24-hour observation. Do not leave valuables or important papers lying around your hotel room.

(2) Do not stay above the sixth floor. Many foreign fire companies do not have ladders that go beyond this floor. The third floor is your best choice. Occupants of rooms lower than the third floor are subject to a higher degree of burglaries or robberies by people entering from the street.

c. Airport and Customs Concerns

(1) Be careful to make an accurate and complete declaration of money (including traveler's checks), credit cards, and all valuables (including cameras and jewelry whether worn or carried). It is imperative to retain a copy of this declaration until departure. Use only authorized banks and currency exchanges.

(2) Security screening process at international airports shall vary depending upon the country visited. Arrive at the airport at least 2 hours prior to departure. This allows for ample time to pass through the security screening process. Do not linger in the airport ticketing area after checking-in. This is the most vulnerable section of the airport and has been the repeated target for terrorist groups. Proceed to the security area as soon as possible. Questions asked by airport security officials may sound like the officer is conducting an interrogation. The officer is looking for indications of possible criminal or terrorist activity. Be cooperative and answer all questions truthfully. Airport security officials may be especially concerned with electronic devices, so travelers should be forthcoming about any in their possession. In Germany, airport officials have been known to request individuals to extract the batteries from the devices before boarding the aircraft. Other countries may have similar policies.

(3) Laptop computers are a focus of security people because they have been used to hide drugs and explosives in the past. Countries in Central and South America and Europe may be particularly concerned with laptop computers. Persons traveling with a laptop should be prepared to demonstrate its functions at all security checkpoints.

d. Crime Prevention

(1) Contact a DAO or Consulate or Embassy Regional Security Officer about the local situation if necessary. Find out which parts of town local inhabitants consider risky. Stay in well lit areas; do not use short cuts or narrow alleys. Be especially alert in crowds. Thieves often strike when travelers are distracted. The most common sites for thefts to occur are tourist spots, shopping areas, transportation centers, and train stations. Dress modestly and be discreet.

(2) Theft is common on overnight trains. Place luggage under the seat rather than on overhead racks. Keep valuables under the pillow or in a safe pack around the neck or waist. If traveling in a group, sleep in shifts.

(3) Men, if possible, should keep their wallet in a front pocket. Frustrate pickpockets by taking the following precautions: wrap rubber bands around the wallet to make it difficult for a pickpocket to remove it, keep the wallet with a comb through the fold with the teeth facing upward so it shall catch on the pocket lining if removed, place a handkerchief over your wallet or place the wallet in your pocket sideways. Women, if possible, don't carry a handbag. They are considered

an "easy target" for thieves. They simply take the bag and run, resulting sometimes in physical injury to the carrier. If travelers need to carry a handbag, do not carry money or identification in it. Hide all valuables on your person. Money belts or pouches worn on the outside of clothing or loosely hung around the neck are easily cut or ripped off. Remember, wearing them on the outside highlights where you keep all your valuables.

(4) In areas noted for carjacking or tourist robberies, make sure rental vehicles do not have special license plates or agency stickers.

(5) When driving, stow belongings in the car's trunk rather than on the back seat. Keep windows up and doors locked. Empty the trunk at night, even if the parking area is guarded.

(6) In the event of a flat tire, drive to a service station or busy intersection before stopping. If the vehicle breaks down, wait inside for assistance from police or an authorized repair person with proper identification.

(7) Be cautious of sexual overtures from anyone. Aside from the potential health hazards, prostitutes are often the decoys who steer you into becoming a victim of other crimes, such as robbery and extortion. From a CI perspective, offers of sexual companionship have historically been a method used by FIS in an attempt to compromise Government employees and Government contractors.

(8) Attempt to know the laws and rules of the country to be visited. Do not engage in black marketing or other illegal activities. Do not engage in black market currency exchanges or other illegal transactions. Depending upon the country's exchange rate, the financial advantage of engaging in such activity may be substantial, but it is not worth the risk.

(9) Do not attempt to propagandize or engage in political arguments. Many foreign nationals are curious about the United States, and are genuinely interested in talking to Americans. Their questions are best answered in an objective forthright manner without drawing unfavorable comparisons with the country visited.

(10) Be careful about accepting invitations. Do not overindulge in drinking or engage in promiscuous activities. Audio (listening) devices and hidden photographic cameras are often planted in rooms. Depending upon the country visited, if invited to a foreign national's residence, or to any other form of private gathering, try to keep at least one other member of your group with you. Travelers should maintain a healthy skepticism toward persons who seem to attach themselves to them. Overly friendly tourist guides, interpreters, or maids, who show an undue interest should put the traveler on the alert. Do not trust interpreters with matters of confidence.

(11) Do not accept letters, personal messages, photographs, packages, or other material to be carried openly or smuggled in or out of the country.

(12) Travelers generally are NOT under individual surveillance during visits; however, if he or she suspects that they are being watched, resist any temptation to "play games" with what may seem to be clumsy attempts to keep an eye on you. Do not attempt to lose real or imagined

surveillance by taking evasive maneuvers, searching your room for listening devices ("bugs"), or attempting to play tricks on such "bugs." This sort of action only serves to arouse suspicion and may result in increased foreign security attention and possibly harassment.

e. General Comments

(1) Do behave in a natural manner, use good judgment, and enjoy the trip.

(2) Maintain a "low profile" by:

(a) Blending in with local populace.

(b) Wearing suitable attire -- do not over or under dress.

(c) Being sensitive to local customs and laws.

(d) Traveling in pairs or small groups of no more than four people.

(e) Using rental rather than official cars if possible.

(f) Not flaunting American citizenship or attaching an "air of importance" to yourself.

(g) Not being aggressive or insulting to the native population.

(h) Ensuring that your itinerary is not publicized, but given to those who have a "need to know."

(3) The following are suggestions for personal safety:

(a) Unobtrusively inspect under seats and seat cushions on airplanes or other modes of transportation.

(b) Inspect the rental vehicle for signs of tampering.

(c) Park and lock car in a secure area.

(d) Avoid lingering in potential threat areas such as general terminal areas at airports or lingering in front of official buildings being visited.

(4) Never pick up souvenirs, statues, or artifacts just because they appear to be lying around or unclaimed. Purchase such items in approved shops only, making certain that a receipt is provided for each purchase. Do not sign any receipts for money or services, unless first assured of and furnished an on-the-spot copy which clearly identifies and itemizes the nature of the transaction.

(5) Do not make or write any statements that might be exploited for propaganda purposes. Do not sign petitions, however innocent they may appear.

(6) Do not photograph any military personnel, equipment, installation, defense plant, or other military or restricted area. Also, refrain from photographing slum areas, ghettos, or underprivileged persons in the host country. Do not photograph airports and train yards or other facilities that could be used for military purposes.

(7) As a precaution, be aware that clothing may be tagged with invisible dyes or radioactive materials. This can be done at a dry cleaning establishment or in your room. If a letter were placed in the tagged pocket and later mailed, it could be retrieved and traced.

(8) In writing letters, use personal stationery and not that given to you by any local hotel. Also purchase stamps at a post office or embassy. Stamps obtained at a hotel or other source can be tagged with invisible inks or radioactive tracers. Assume that letters shall be opened and read. If necessary to write about confidential matters, use appropriate channels of the Embassy or Consulate.

(9) If detained, remember, tourists generally have nothing to worry about so long as they follow the local rules, and use good judgment. However, occasionally individuals do encounter trouble with authorities; either by mistake, or as the result of some injudicious action. Should this occur, the most important things to remember are:

(a) Insist on being put in contact with the American Consulate at once. If the authorities stall or attempt to intimidate, refuse to make any statement until this has been done. Experience shows that if an individual cannot be intimidated by vague or implied threats, the detainer shall usually back down if the individual has not, in fact, done anything wrong.

(b) Under no circumstances sign any document until you have had the opportunity to meet with a U.S. official.

(c) Remain calm, but assertive. Do not antagonize Government officials, but continue to insist on your right to speak with a representative of the U.S. Government.

f. Hostage Situations. In the event of a hostage situation:

(1) Do not physically resist, but passively cooperate with captors.

(2) Prepare mentally for a long period of hostage negotiations.

(3) Remember that although negotiations are usually lengthy, virtually all hostages are released unharmed.

(4) Attempt to establish personal rapport with your captors, while at the same time maintaining personal dignity.

(5) Do not become involved in controversial discussions with the terrorists.

(6) When a rescue party approaches, lie on the floor with your hands covering your head; do not move until instructed to do so by members of the rescue team.

g. Air Travel. Military air or military/Government charter flights are preferred within CONUS. Non-stop commercial transcontinental flights are considered more vulnerable to possible hijacking than those making intermediate stops. Outside CONUS, every effort should be made to fly via military aircraft, diplomatic courier flight or military/Government charter flight. Commercial air travel aboard U.S. flag aircraft that does not have intermediate, weather, alternate or landing rights in "threat areas," or areas of high vulnerability to hijacking is recommended.

h. Hijackings. If U.S. military or Government civilian personnel should happen to be aboard an aircraft that has been hijacked:

(1) If in uniform:

(a) Be as unobtrusive as possible.

(b) Do not attempt to take charge, demand privileges of rank, or openly advise other passengers as to their conduct.

(c) If asked for identification, show only passport (tourist if possible).

(2) If in civilian clothing, do not offer to make known a U.S. military or Government affiliation unless forced to do so. Most persons previously placed in such a situation have been requested only to show some reasonable identification (e.g., driver's license, passport, credit cards).

(3) The traveler must keep in mind that, these are only "guidelines," not "hard and fast" regulations that apply in all situations. The world and the rules have changed since 9/11. There are no guarantees. In all situations be adaptive and flexible.

7. REPORTING PROCEDURES. If you suspect an approach has been made, or you become involved or entrapped in a conspiracy to commit espionage, you are to report to the nearest U.S. Consulate, Attaché, Embassy Regional Security Officer or Post Duty Officer. If you have been indiscreet or otherwise compromised, he or she shall discuss the situation in confidence with a U.S. security representative. Above all, do not attempt to get out of an embarrassing situation by yourself, or assume the role of a self-appointed counterintelligence agent.

8. ADDITIONAL INFORMATION. Any suspected approach made subsequent to travel should be reported through the traveler's security officer or commander to the appropriate counterintelligence organization.

ENCLOSURE 3

INDUSTRIAL SECURITY

1. FACILITY CLEARANCE (FCL). A FCL is a determination by the Defense Security Service (DSS) that a contractor facility satisfies the requirements for access to classified information. Requirements for obtaining a FCL are outlined in DoD Manual 5220.22, Volume 2 (Reference (u)). Although contracts requiring contractor access to classified information may be awarded to contractors that do not yet possess a FCL, execution of those contracts does require the appropriate FCL. The contractor must be sponsored for an FCL by a Government agency or another contractor, who can sponsor a subcontractor for an FCL.

2. FCL FOR CONTRACTORS. Contractors may bid for and the Government may issue contracts requiring contractor access to SCI information prior to the contractor obtaining a FCL. However, access to SCI information shall not be authorized to individuals performing under such a contract until a final FCL has been processed in accordance with paragraph 4 of this enclosure and personnel security clearances for the contractor employees have been obtained in accordance with paragraph 5 of this enclosure.

3. FCL REQUIREMENTS FOR ACCESS TO SCI. Contractor personnel may not be permitted access to SCI based on an interim TOP SECRET FCL.

a. The DoD Component or agency must have a valid contractual requirement to sponsor the contractor for a TOP SECRET FCL for access to SCI.

b. The contractor company must possess a final TOP SECRET FCL.

c. The CSSO must meet SCI eligibility requirements and be indoctrinated for SCI.

d. Contractor employees, to perform work on SCI contracts, must meet SCI eligibility requirements and be indoctrinated for SCI.

4. CONTRACTOR AND CONSULTANT PERSONNEL SECURITY CLEARANCE (PCL) REQUIREMENTS

a. Contractors. See Enclosure 2 of this Volume.

b. Consultants. A consultant to a Government agency may be authorized access to TOP SECRET SCI based on a properly adjudicated PCL provided that individual meets the following requirements:

(1) Is self-employed.

(2) Does not employ or partner with any other individual.

(3) Has been nominated to perform work under contract that requires access to SCI material.

c. Contracting Officer's Representative/Contract Monitor (COR/CM). The COR/CM must be a Government employee (military or civilian) who is appropriately cleared and SCI indoctrinated for all accesses required by the contract. An alternate COR/CM should be appointed to assist the COR/CM whenever the COR/CM is not available.

d. SCI Contract Process. The COR/CM must ensure that the delegated HICE, Senior Intelligence Officer (SIO), or the cognizant SSO is included in the SCI contract process. (The SIO exercises overall management of SCI programs under the SIO's security cognizance; however, the cognizant SSO usually executes management.)

5. CONCEPT VALIDATION FOR CONTRACTOR SCIFs

a. In addition to the requirements outlined in Enclosure 2 of Volume 2 of this Manual, a properly executed DD Form 254 must accompany the concept validation request for the construction of a SCIF at a contractor facility.

b. The DD Form 254 must identify SCI-safeguarding requirements and performance at the contractor location, and the place of performance identified in block 8.a. of the form must be the same location identified on the fixed facility checklist (FFC).

c. The SSO of the DoD Component that has established the contract must review and approve the DD Form 254. Submission of a concept validation for a contractor SCIF must include a certification from the SSO that the contractor has a Final TOP SECRET FCL, or a TOP SECRET FCL has been requested from DSS.

d. Contractor companies that do not possess a final TOP SECRET FCL shall not be eligible to receive a final SCIF accreditation until receipt of the final TOP SECRET FCL and personnel security requirements outlined in paragraph 5 of this enclosure have been met. However, the concept to construct a SCIF may be reviewed and approved by DAC prior to DSS issuing a final TOP SECRET FCL.

e. Upon receipt of the final TOP SECRET FCL and after personnel security requirements have been met, the Government sponsoring SSO shall notify DAC, which shall accredit the SCIF in accordance with Enclosure 2 of Volume 2 of this Manual.

6. STORAGE REQUIREMENTS FOR SCI AT THE CONTRACTOR FACILITY. See Enclosure 2 of Volume 2 of this Manual.

7. CONTRACTOR RESTRICTIONS. Contractors who have TOP SECRET/SCI access may have unescorted access to a Government facility and may be permitted to work alone inside the facility without the requirement of the presence of a U.S. Government employed representative provided all proprietary information (PROPIN) is secured to preclude unfettered contractor access to this material. This restriction applies to Government-owned, contractor-operated (GOCO) facilities as well.

8. ACQUISITION RISK DIRECTORATE (ARD), NATIONAL COUNTERINTELLIGENCE EXECUTIVE. Consistent with local agency policy, industrial security specialists (ISSs) may contact their agency representative at ARD for an assessment of any contractor or subcontractor obtaining a new contract that requires contractor access to classified information. ISSs should refer to Director of Central Intelligence Directive (DCID) 7/6 (Reference (v)) for additional information regarding ARD assessments. Upon receipt from ARD, the ISS shall forward the assessment to the contracting officer prior to the award of a contract. The contracting officer shall make a risk assessment of the contractor based on type and scope of work, threat level, and other information, and either award or deny the contract to the contractor.

9. INSTALLATION OF JWICS AT A CONTRACTOR SITE. DoD 5105.21 (Reference (w)) establishes DIA as the DoD Executive Agent for JWICS and JWICS supported systems. DIA retains full responsibility for the secure operation of the system, connectivity, and the protection of classified information on the system. DIA may require installation of specific equipment to support the JWICS installation and connectivity. Cost of installation of JWICS is the responsibility of the department or agency that identified the need for contractor access to JWICS at the contractor site. A contractor may have access to JWICS at the contractor site provided all the following conditions have been met. These requirements cannot be waived or mitigated:

a. The statement of work or statement of objectives must specify a continual ongoing requirement for access that cannot utilize other means of information transmission or exchange.

b. The contractor facility must possess a FINAL TOP SECRET FCL.

c. The DD 254 must require installation and connectivity of JWICS at the contractor site.

d. The DD 254 must require the contractor to have a communications security (COMSEC) account. The extension of a COMSEC account assigned to a department or agency, to a contractor facility is prohibited.

e. The contractor must develop a concept of operations for the installation, protection, and use of JWICS at the contractor facility and submit it through their contracting officer or COR to the DIA/JWICS Program Management Office and DIA/SYS-4 for review and approval.

f. The HICE or designee must obtain written permission from the originators of PROPIN information prior to the installation of JWICS if the contractor shall be permitted to receive this information or to access systems that contain this information.

g. Once approval from DIA is received, installation may be initiated and upon review by DIA of the installation requirements, connectivity may be issued.

ENCLOSURE 4

SCI ACCESS FOR THE EXECUTIVE, LEGISLATIVE, AND JUDICIAL BRANCHES

1. EXECUTIVE BRANCH ACCESS. The President, Vice President, and Cabinet officers have access to SCI materials. The DNI is responsible for their appropriate security indoctrination. The DNI may grant access to such other persons who shall require SCI access to perform their duties, subsequent to appropriate security indoctrination briefing. Accordingly, DoD HICE may grant the President, Vice President, Secretary of Defense, Deputy Secretary of Defense, and the DNI access to SCI materials without a clearance message.

2. LEGISLATIVE BRANCH ACCESS

a. Policy. All legislative branch access to SCI shall be conducted in accordance with Reference (d). As a basic principle, access to intelligence information shall be consistent with the protection of intelligence sources and methods. Normally, congressional requests for intelligence information can usually be satisfied at the collateral level, but, in certain instances, there may be a need for access to SCI. In these instances, every effort shall be made to exclude, to the extent possible, data on intelligence sources and methods.

b. Members of Congress. Members of Congress may be provided access to SCI on a need to know basis without a security investigation or adjudication after the appropriate indoctrination. HICEs or program managers providing SCI shall administer indoctrination briefings on the sensitivity and vulnerability of the information, and the sources and methods involved as required to maintain proper protection.

c. Committee Staff Members. Access to SCI by staff members of the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) are governed by memorandums of understanding executed by the chairmen of these committees and the DNI. Provision of information and materials to these committees shall be in accordance with mutually agreed arrangements between the SSCI and HPSCI chairmen and the DNI.

d. Other Personnel. Requests for SCI access approvals for other legislative branch personnel shall be referred to the Director of Legislative Affairs, ODNI, for approval. Requests must be in writing by committee or subcommittee chairmen and clearly describe the nominee's need to know. Issues arising with regard to particular requests shall be referred to the DNI for resolution. Unless otherwise authorized by the DNI, approval for SCI access for legislative branch staff personnel shall be limited to:

(1) Permanent staff personnel of appropriate congressional committees and subcommittees.

(2) Selected employees of the Government Accountability Office and the Library of Congress.

(3) Selected members of the staffs of the leadership of the House and Senate, as agreed by the DNI and the leadership.

e. Verification Requirement. The DNI's Office of Legislative Affairs shall verify, in coordination with program managers and on behalf of the DNI, the need of persons in the legislative branch, other than members of Congress, for SCI access. Verifications shall be based on such persons' job responsibilities in the following areas:

(1) Direct involvement in authorization legislation pertaining to IC organizations.

(2) Direct involvement in appropriations legislation for IC organizations.

(3) Direct involvement in reviews authorized by law of activities of IC organizations.

(4) Direct involvement in other legislative matters which, of necessity, require direct SCI access.

f. Access Approval Procedures

(1) SCI access approvals may be granted to staff personnel in the legislative branch, described above, who possess a TOP SECRET collateral clearance and who meet the investigative standards set forth in Reference (l). Requests for exceptions to this policy shall be referred to the DNI's Office of Legislative Affairs. The requester of the SCI access approval is responsible for having a Single SSBI conducted. Adequate records of investigation and clearances should be kept and updated. Reports of investigations shall be reviewed by the DNI's Director of the Special Security Center to assure uniform application of Reference (l) security criteria. The granting of access approvals shall be coordinated with the appropriate program managers, as agreed by the DNI.

(2) Staff personnel in the legislative branch receiving SCI access approvals shall be provided appropriate security briefings by the ODNI Special Security Center and shall sign NdSs before receiving SCI access. SCI access approvals shall be recorded in the Scattered Castles database. Copies of NdSs shall be provided to program managers who request them.

(3) The DNI Office of Legislative Affairs shall be notified promptly of employee job changes or terminations so that employees who no longer require access are debriefed and the community wide data base is updated. SCI access approvals for legislative branch employees must be withdrawn if an employee leaves the specific position for which access was authorized. If SCI access is required in the new position, a new need to know determination by the ODNI Special Security Center is required.

(4) SCI shall be made available to committee and subcommittee members only through or under the authority of the Chairman of the Congressional committee or subcommittee concerned.

g. Handling and Storage of SCI

(1) Hardcopy Documents. The executive branch component providing SCI to Congress shall ensure that the handling and storage of such information conforms to the requirements of Intelligence Community Standard (ICS) 705-1 (Reference (x)) or successor policy statements. Legislative branch SCIFs are accredited by the CIA and should be verified with CIA's Office of Security. Where adequate provisions cannot be made for the handling and storage of SCI, SCI shall not be provided without the approval of the DNI.

(2) Testimony or Briefings. When presenting testimony or briefings involving SCI to persons in the legislative branch, use the following security measures:

(a) Thorough physical security and TSCM inspections shall be conducted in accordance with Reference (v) and ICD 702 (Reference (y)).

(b) All persons present, other than elected officials, including transcribers and other clerical personnel, must be certified for access to the SCI being discussed. Congressional security offices shall make arrangements to monitor entrances to the room where the presentation shall be given to exclude unauthorized persons.

(c) All transcriptions or notes that result from briefings or testimony must be handled and stored according to the SCI security requirements in Reference (x).

(d) The room in which a presentation is given must be inspected after the presentation to properly secure all SCI.

(e) Any IC element providing SCI to a congressional committee, other than a committee routinely involved in the oversight and appropriations processes of IC organizations shall endeavor to provide such information through the SSCI or HPSCI, as appropriate. The SSCI and HPSCI both have facilities that meet Reference (x) requirements and personnel trained in SCI handling procedures. The committee requesting the information shall contact the HPSCI or SSCI and obtain their permission to use their facilities prior to the transmittal of the information. Where possible, the custody of such information shall remain with the IC organization concerned. Where such information must be physically transferred, arrangements shall be made between the providing organization and congressional security officials beforehand to eliminate or minimize the risk of exposure of SCI sources and methods. Records of the transfer shall be maintained by the department or agency providing the information.

h. Marking SCI Released to Congress. SCI being prepared for release to members of Congress and Congressional committees shall be marked with all applicable classifications, SCI caveats, codewords, project indicators and dissemination control markings. The term "SENSITIVE" may not be used instead of, or in addition to, SCI markings, as it does not convey

the nature or extent of the sensitivities involved. Congressional security officials shall ensure that the congressional committee staff employees, and employees of the Library of Congress and the Government Accountability Office, have clearances and SCI access authorizations appropriate for receipt of the material involved.

i. Release of SCI Material to Congress

(1) Process intelligence information for release to Congress in accordance with DoDD 5400.4 (Reference (v)) and this Volume.

(2) Make maximum use of existing sanitization and decompartmentalization authority in preparing testimony and documentation for Congress.

(3) The appropriate HICE and Legislative Liaison Office are the offices of primary responsibility for determining that congressional committee staff employees and employees of the Library of Congress and General Accounting Office have the appropriate security clearances and access(es) for receipt of the material involved. DoD Components that provide SCI to the legislative branch or its components must forward the SCI material through the appropriate HICE for control and transfer to an accredited SCI facility.

(4) Upon notification from the appropriate Legislative Liaison Office of a pending visit by a member of the legislative branch, the HICE shall certify all appropriate access certifications pertinent to the visit. This SCI access certification shall also contain guidance on SCI release.

(5) The cognizant SSO or SIO must review formal witness statements or briefings that contain or may contain SCI for proper security markings prior to forwarding to the appropriate HICE for staffing.

(6) Congressional SCI transcripts shall be reviewed by congressional security officials with input from office of the HICE providing the information. The HICE that originally provided the SCI information may identify an office of primary responsibility within his or her element that shall coordinate the sanitized response.

3. JUDICIAL BRANCH ACCESS

a. All judicial branch access to SCI shall be conducted in accordance with Reference (d).

(1) Federal Judges. Federal District and Circuit Court Judges and Supreme Court Justices are the only judicial branch employees exempt from routine security clearance processing. All other judicial branch personnel must receive a security clearance as provided for in Reference (q) and be granted SCI access and receive an SCI indoctrination briefing by a Department of Justice (DOJ) Security officer.

(2) Other Judges. Magistrates, immigration commissioners, administrative law judges, hearing commissioners, and other such court officials, must undergo an SSBI investigation and SCI adjudication prior to access.

(3) Court Personnel. All other court, Government, and support personnel (law clerks, attorneys, U.S. Marshals, courtroom clerks, court reporters, administrative officers, secretaries, etc.) who have a validated need to know must obtain SCI access authorization from the DOJ Security Official.

(4) Defense Personnel. The Government may obtain, consistent with CIPA and its security procedures, as much information as possible in its attempt to make an adjudication for temporary access to SCI pursuant to Reference (k) for those individuals acting for the defense.

(5) Jury. There is no requirement for investigation or SCI access authorization for members of Federal juries. At a minimum, the Government shall request the trial judge to give jurors a cautionary instruction on disclosure of classified information provided during the trial.

(6) Court Security Officer. A Judicial Security Officer (JSO) shall be appointed by the Court from recommendations submitted by the DOJ Security Officer and with the concurrence of the HICE(or designee) from which the case-related SCI originates. The JSO is responsible for ensuring compliance with CIPA and all other applicable directives and regulations concerning the safeguarding of SCI, and for providing needed SCI security support to all persons involved in particular cases.

b. SCI Access Requirements. Requirements for SCI access shall be provided to the JSO who shall notify the DOJ Security Officer. The DOJ Security Officer shall coordinate requirements with agencies or program managers involved.

c. SCI Access Eligibility Determination Procedures. SCI access shall be authorized by the DOJ Security Officer, who is responsible for adjudicating the results of investigations against eligibility criteria outlined by Reference (k).

(1) The court, and other appropriate officials, shall be notified in writing by the DOJ Security Officer of SCI access approvals.

(2) SCI indoctrination briefings shall be provided by DOJ Special Security Center (SSC) personnel, or by an appropriately indoctrinated representative of the DOJ SSC.

d. Handling and Storage of SCI

(1) Pursuant to section 9 of Reference (d), the DOJ Security Officer, in coordination with the appropriate IC agency security representative, is responsible for arranging for the care, custody, and control of SCI material involved in any Federal criminal case.

(2) Questions concerning the interpretation of the CIPA shall be resolved by the court in consultation with the DOJ Security Officer and the appropriate IC agency's security representative.

ENCLOSURE 5

SECURITY INCIDENTS

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

2. SECURITY INCIDENTS. It is the responsibility of all SCI-indoctrinated personnel to report any security incidents affecting or involving SCI to the appropriate SSO or local SCI security official. Security managers shall ensure all security violations and incidents involving SCI information are reported immediately to the appropriate SSO. An appropriate report shall be prepared and provide sufficient information to explain the incident. Security incidents are categorized as either violations or infractions.

a. Security Violations. A security violation is a compromise of classified information to persons not authorized to receive it or a serious failure to comply with the provisions of security regulations or this Manual and which is likely to result in compromise. A security violation requires investigation.

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

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

b. Infractions. An infraction (formerly known as a “practice dangerous to security”) is a failure to comply with the provisions of security regulations or this Manual or any other action that causes a potential compromise of classified information.

(1) An infraction requires immediate corrective action but does not require investigation. An infraction does not constitute a security violation but can lead to security violations or compromises if left uncorrected. Examples of infractions include, but are not limited to, a courier carrying classified documents stopping at a public establishment to conduct personal business, or placing burn bags adjacent to unclassified trash containers.

(2) Management officials shall take prompt corrective action on any reported infraction and document the actions taken.

3. REPORTING PROCEDURES. Report all security incidents involving SCI to the appropriate SSO or local SCI security official.

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

b. For a security violation with a determination of "Compromise Certain" (see subparagraph 4.c.(1) of this enclosure), the cognizant HICE shall immediately report the incident to the appropriate IC program manager and send a copy of the report to DAC. An investigation shall be conducted to identify full details of the violation or compromise, and to determine what specific information was involved, what damage resulted, and whether culpability was involved in the incident. Investigations shall be reported through the chain of command to the CSA.

c. The HICE shall provide summaries of investigations to the DNI through the ODNI Special Security Center or successor office with a copy to DAC in accordance with ICD 701 (Reference (aa)) under the following conditions:

(1) Unauthorized disclosure to an international organization, foreign power, agent of a foreign power, or terrorist organization.

(2) National intelligence activities or information that may be at risk of appearing in the public media, either foreign or domestic, without official authorization.

(3) Loss or compromise of classified information that poses a risk to human life.

(4) Loss or compromise of classified information that is indicative of systemic compromise.

(5) Loss or compromise of classified information storage media or equipment.

(6) Discovery of clandestine surveillance and listening devices.

(7) Loss or compromise of classified information revealing U.S. or a foreign intelligence partner's intelligence operations or locations, or impairing foreign relations.

(8) Such other disclosures of classified information that could adversely affect activities related to US national security.

(9) Loss or compromise of classified information revealing intelligence sources or methods, US intelligence requirements, capabilities and relationships with the U.S. Government.

d. Local SCI security officials shall advise the parent command SCI security officials of SCI security violations occurring within their security cognizance and involving personnel assigned to that parent command.

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

(1) The SSO notifies both organizations of the security violation.

(2) The organization with security cognizance shall conduct an investigation.

(3) A report of investigation is forwarded to both organizations.

(4) The organization whose activity committed the violation shall determine what corrective action should be taken. The report of this determination shall be forwarded to the other organization involved.

f. All security violations occurring on computer systems, terminals, or equipment which process SCI shall be reported through command SCI channels to the appropriate HICE with information copies to DAC. SCI security officials and the site information assurance manager should coordinate security incidents involving computers. Computer security incidents shall be reported to the DNI in accordance with ICD 503 (Reference (ab)). Examples of serious computer security incidents include, but are not limited to:

(1) Human error in reviewing media for content and classification, resulting in compromise.

(2) Incorrect setting of a security filter that results in the compromise of intelligence.

(3) Intrusion attempts, either physical or through hacking.

(4) Virus attacks.

(5) Failure of a system or network security feature.

g. Commanders, supervisors, and their security officials must report SCI security violations or other information that could impact an individual's continued eligibility for access to SCI to the appropriate CSA and the appropriate central adjudication authority.

4. INQUIRIES AND INVESTIGATIONS

a. Preliminary Report of Inquiry. When the SCI security official determines that a security violation has occurred, the SCI security official must report the violation within 72 hours of discovery to the appropriate HICE or designee with information copies to DAC. (See Figure 7 in

Appendix 1 to this enclosure for sample report format.) The SIO must appoint an inquiry official. Preliminary inquiries shall not be conducted by the SSO or staff member. The SSO shall brief the appointed inquiry official concerning the conduct of the official inquiry. The SSO shall provide status reports to the SIO and an information copy to DAC every 30 days until the final report is submitted. Classify reports of inquiry according to content. The inquiry official shall provide a final written report of inquiry to the SIO through the SSO. The SIO shall refer the incident for formal investigation when the final report of inquiry finds there is a reasonable likelihood of compromise of SCI.

b. Investigation Procedures. Investigations shall determine if there is a reasonable likelihood that a compromise of SCI may have occurred, the identity of the person(s) responsible for the unauthorized disclosure, and the need for remedial measures to preclude a recurrence. The investigation should reveal the following information for each separate action or movement of SCI material from the time the violation started until it was discovered and corrected. Investigations reports (see Figure 8 in Appendix 2 to this enclosure) should include:

(1) Who was involved (both SCI-indoctrinated and non-SCI-indoctrinated).

(2) What specifically took place during each action or movement.

(3) When each separate action or movement began and ended.

(4) How the actions or movements took place (i.e., relate each action to the preceding and following actions).

(5) Where each action happened (i.e., trace the route that SCI material followed during the violation). If the sequence of events cannot be determined by investigating from present to past, investigate from past to present. However, an investigation from past to present is less desirable, because distortion of events is more likely.

c. Compromise Determination. The investigator shall make a compromise determination, using facts obtained during the investigation, for each security violation to be included in the final report, based on the following categories.

(1) Compromise Certain. SCI has irretrievably left SCI control channels; uncontrolled dissemination can be confirmed. Examples include a violation in which SCI appears in a newspaper or other public media, or SCI is known to have been seen by a foreign national or non-SCI accessed U.S. citizen, who there is reason to believe shall not protect the information. When a SCI eligible non-indoctrinated person views SCI, the security violation shall not be considered a certain compromise if there is reason to believe the information shall be protected. See subparagraph 4.c.(2) of this enclosure.

(2) Compromise Probable. SCI has left SCI control channels; uncontrolled dissemination may reasonably be expected to occur, but a specific threat cannot be identified. For example, an SCI document found laying on a busy street would be a probable compromise because there is no way of knowing if anyone saw the document. Cases in which the

investigator suspects SCI has been exposed to unauthorized personnel, but believes that further inquiry shall only draw undue attention to the information, is also a probable compromise. An example of this situation is the discussion of SCI information in the presence of non-SCI-indoctrinated individuals. In this instance, the administration of inadvertent disclosure agreement would be appropriate. The transmission of SCI in an unclassified general service (GENSER) message, on IT systems or other electronic media devices given worldwide distribution could also fall into this category.

(3) Compromise Possible. The possibility of uncontrolled dissemination of SCI cannot be ruled out, but with no specific indication to believe such dissemination shall take place. A lost document containing SCI or SCI materials found in a non-secure location may represent a possible compromise. Transmission of SCI in a GENSER message might also fall into this category if distribution was limited, if the message were classified either SECRET or CONFIDENTIAL, if SCI were placed on an internal, non-Internet connected IT system, or if the SCI is unlikely to be recognized.

(4) Compromise Improbable. These are cases in which uncontrolled SCI dissemination is unlikely, but cannot be positively ruled out. This category includes exposure of SCI to unauthorized persons where an inadvertent disclosure agreement has been executed, or where the personnel exposed are SCI eligible, but not indoctrinated for the material. Compromise improbable also includes cases in which the investigator is satisfied that an unauthorized person is not aware of exposure or is unlikely to remember the SCI material; where SCI material is sent through the U.S. Postal System but the material is double wrapped, the packaging shows no sign of tampering, and the material is delivered without undue delay. Another example is a case where it is improbable, but not certain, that the material ever left SCI control channels.

(5) Compromise None. It is certain that SCI did not leave SCI control channels and was not exposed to unauthorized personnel. SCI found unsecured in a SCIF not authorized open storage may fall into this category. Compromise none also applies to individuals who have a valid TOP SECRET clearance, are indoctrinated for a category of SCI, and are inadvertently exposed to one or more SCI categories for which they are not indoctrinated.

d. Final Report. Reports of investigation shall include sufficient detail to explain the incident. (See Appendix 2 to this enclosure for sample format.) The report shall assess intent, location of incident, risk of compromise, sensitivity of information, and mitigating factors in arriving at a final analysis of the incident. Final reports of investigations, to include those conducted in accordance with the Uniform Code of Military Justice (Reference (ac)), shall be forwarded through the SCI chain of command to the CSA.

5. CORRECTIVE ACTION

a. The appropriate SCI security official shall review the final report, advise the cognizant HICE or designee of weaknesses in security programs, and recommend corrective action. HICEs or designees are responsible to take appropriate corrective action in all cases of actual security violations and compromises. Administrative sanctions imposed in cases of demonstrated

culpability shall be recorded in security files of the responsible SCI security official. Except in instances where immediate action is necessary, an individual found responsible for a security incident shall be afforded the opportunity to present information in their defense prior to the implementation of administrative sanctions. Remedial sanctions according to the severity of the incidents may be applied by the HICE or designee.

b. Security deficiencies identified by investigation which contributed directly to the incident shall be corrected if it is within the capability of the HICE concerned. If not, full details and recommendations on corrective measures shall be provided to DAC.

6. CLASSIFICATION REVIEW

a. If SCI information has been compromised or subjected to compromise, the original classification authority shall reevaluate the classification and decide whether to:

(1) Continue classification without changing the information.

(2) Modify the specific information, or parts thereof, to minimize or nullify the effects of the reported compromise and retain the classification.

(3) Downgrade the information.

(4) Upgrade the information.

(5) Declassify the information. Lost or compromised documents should be considered for declassification to the fullest extent compatible with national security.

b. The original classification authority shall notify the appropriate SCI security official of the results of the evaluation (see Figure 9 in Appendix 3 to this enclosure). If any change is made to the classification of the information, the originator shall promptly advise all holders of the information.

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

7. DAMAGE ASSESSMENTS

a. Refer notices of compromise or requests for damage assessment to the appropriate HICE or designee for action. (For organizations under SSO DIA cognizance, refer actions to SSO DAC.) The HICE or designee shall review the notice or request and task the appropriate element for a damage assessment, if required. Coordinate cases involving legal action with the appropriate General Counsel or Staff Judge Advocate.

b. The damage assessment shall consider how the loss or compromise of the SCI material could result in damage to U.S. national security interests. Expeditious damage assessment is essential to the success of the program. The damage assessment is used to:

(1) Reevaluate lost or compromised information.

(2) Determine if any changes in classification are appropriate.

(3) Indicate damage to the national security.

8. CASE FILE RETENTION. Retain case files referred to the Department of Justice or DoD for prosecution determination for 5 years after the closure of the case. Retain all other case files for 2 years after completion of final action or when no longer needed, whichever is sooner.

9. INADVERTENT DISCLOSURE AGREEMENTS

a. The local SCI security official shall exercise his or her best judgment to maintain SCI security by seeking written agreements from non-indoctrinated persons to whom SCI was inadvertently disclosed (see Figure 5). Inadvertent disclosure agreements must be signed by the individual entering into the agreement and by a witness who can affirm that the signing individual read the agreement form. An inadvertent disclosure briefing (see Figure 6) should be given to non-indoctrinated persons exposed to SCI contemporaneously with the presentation of the inadvertent disclosure agreement.

Figure 5. Inadvertent Disclosure Agreement

INADVERTENT DISCLOSURE AGREEMENT

I hereby affirm that I have read and that I understand the above instructions for maintaining the security of certain sensitive intelligence. I certify that I shall never divulge the classified information inadvertently exposed to me, and I shall not reveal to any person my knowledge of the existence of such information. I understand transmission or revelation of this information in any manner to an unauthorized person is punishable under sections 793 and 794 of title 18, United States Code or appropriate articles of the Uniform Code of Military Justice. I further certify I shall never attempt to gain unauthorized access to such information. My signature below does not constitute an indoctrination or clearance but acknowledges my understanding of the above.

Figure 6. Inadvertent Disclosure Briefing

INADVERTENT DISCLOSURE BRIEFING

1. Information of sensitive intelligence, the source of which cannot be disclosed, has been either discussed with you or exposed to your view. This disclosure was unintentional. It is therefore necessary to acquaint you with the law on this subject and for you to execute a statement binding you to secrecy in connection with any information you may have gained from this disclosure.

2. It is impossible to over-emphasize the importance of safeguarding this intelligence. The time limit for safeguarding of such intelligence never expires. It is directed, therefore, that all reference to the existence of this information, or to words which identify it, be strictly avoided. Transmission or revelation of this information in any manner to an unauthorized person is prohibited by sections 793 and 794 of title 18, United States Code.

3. Although you inadvertently gained information not intended for you, your signature on the attached statement does NOT constitute an indoctrination or clearance for such intelligence.

b. If the person signs an inadvertent disclosure agreement and the responsible local SCI security official has reason to believe that the person shall maintain absolute secrecy concerning the SCI involved, the report of investigation may conclude that no compromise occurred. Copies of executed inadvertent disclosure agreements should be retained as part of the Report of Investigation.

10. DAMAGED DEFENSE COURIER SERVICE PACKAGES

a. If packages are received in damaged condition from the Defense Courier Service (DCS), the receiver shall send an electrical message to the originator and include the following information. If compromise appears possible, the receiver shall also notify the appropriate security official.

(1) Package number and organization from which received.

(2) Specific material involved as well as an inventory of all material contained therein.

(3) Possible cause and extent of damage. Include opinion concerning adequacy of packaging.

(4) Whether or not compromise of material occurred.

b. The receiver shall notify the Commander, DCS, via immediate GENSER message, whenever SCI material delivered via DCS is either lost, damaged, compromised, destroyed, or mishandled. Include a statement giving the SCI classification level of the material. Do not, however, identify the specific material.

11. REPORTING MISSING PERSONNEL. All personnel who have current SCI access or past access to SCI who are killed, captured or missing in action, absent without leave, or similar circumstances shall be reported to the HICE by priority message. In addition to the individual's name, rank, Social Security Account Number (SSAN), and organization, provide a listing or summary of information that may be compromised. Individuals who are killed in action, except SCI couriers or those participating in unauthorized hazardous activities, need not be reported when it is known that death was instantaneous and no possible interrogation could have occurred.

12. REPORTING SCI APPEARING IN THE PUBLIC MEDIA. SCI-indoctrinated personnel should not comment on, confirm, or deny information from open source articles or discussions of an SCI nature. The publication of SCI in the public media does not constitute declassification, decompartmentation, or relaxation of SCI security policy. Acknowledging information of an unauthorized nature can add to the damage or lend credibility to the information.

a. SCI security officials shall report through command SCI security channels to the appropriate HICE or designee and DAC the publication of actual or apparent classified intelligence information in the public media. For incidents involving contractor information or programs, CSSOs shall report through the COR to the appropriate SCI security official.

b. Classify the notification according to content, but at least CONFIDENTIAL, to prevent further possible disclosure. Send the notification by priority Defense Special Security Communications System (DSSCS) message or other secure channel and provide the following information.

(1) Type of medium (e.g., book, newspaper, magazine, television, internet), date of medium, title or headline, and name of author.

(2) Classified intelligence disclosure. Provide a brief synopsis of information disclosed by public medium (the published information itself should not be transmitted). Identify the classification source of the material.

c. The publicly disclosed item (article, book, broadcast transcript, etc.) should not be marked to indicate in any way that it contains SCI. Do not discuss the article outside a SCIF.

Appendixes
1. Preliminary Report of Inquiry
2. Security Violation Investigation Report
3. Classification Review

APPENDIX 1 TO ENCLOSURE 5

PRELIMINARY REPORT OF INQUIRY

Figure 7. Preliminary Report of Inquiry Format

Date

SUBJECT: Preliminary Inquiry into Security Violation - (Date of Violation)

THRU: (Appointing Officer)

TO: Local SCI Security Official

1. Investigating Officer. Name and organization of the investigating officer.

2. Authority. Refer to all appointment memoranda and attach as an enclosure.

3. Matters Investigated. A general statement as to the nature and circumstances of the violation to include a description of the classified material involved.

4. Facts. A brief listing of all pertinent facts pertaining to the violation. Enclose a copy of the violation report, sworn statements, documentary evidence, exhibits, and so forth, as appropriate.

5. Discussion. A brief discussion of the inquiry to include identification of persons interviewed, investigative techniques used (if appropriate), rationale used to reach conclusion, and any other information which is needed for a reviewer to understand the basis for the conclusions and recommendations.

6. Conclusions. A statement as to the conclusions reached. Must include comments as to possibility of compromise and provide the investigator's best judgment regarding the identity of the person(s) responsible for the violation.

7. Recommendation. A statement about procedural or administrative changes that should be made to preclude further violations. If none are required, it should be so stated. No statement should be made by the investigating officer with regard to punitive action against the individual(s) responsible for the violation. An investigating officer's function is to determine and report facts and make recommendations for actions needed to prevent future violations of the type investigated. Disciplinary or punitive action is the responsibility of the appropriate management official, and comments pertaining to such action shall appear in the supervisor's endorsements.

(SIGNATURE OF INVESTIGATING OFFICER)

APPENDIX 2 TO ENCLOSURE 5

SECURITY VIOLATION INVESTIGATION REPORT

Figure 8. Security Violation Investigation Report Format

Date

SUBJECT: Results of Security Violation Investigation: (assigned case number)

THRU: (Appropriate chain of command)

TO: SSO DoD/DIA

1. Summary. A summary of who, what, when, where, why, and how the violation occurred.

2. Sequence of Events. A detailed sequence of events tracing the security violation from start to finish. This sequence shall include a list of all personnel (include name, grade, SSAN, position, organization, clearance level, and access authorized) involved and their specific time of involvement.

a. Indicate date of violation's discovery. Identify the SCI documents or information involved in the violation. Identify individuals not cleared for SCI and the extent of exposure. Identify procedural problems that may have contributed to the violation.

b. Provide a detailed description of the information involved in the incident including classification and compartment levels; controlling headquarters (i.e., originating office and controlling office); and identification of the material (i.e., message, letter, staff study, imagery, and magnetic media) to include document control numbers.

c. Make a statement as to the likelihood of compromise. If material has been compromised, identify the extent of compromise. Identify individual(s), Social Security account number, and office, of personnel at fault for the violation and reason(s) they are at fault.

d. Identify procedure(s) at fault and describe how they led or contributed to the violation.

3. Actions Taken. List actions that have been taken (i.e., messages sent, counseling of individuals involved, and other information as required).

4. Recommendations. Make recommendations concerning what should be done to preclude future violations of this type.

5. Investigating Officer. Investigating officer's name, organization, and telephone numbers.

6. Evaluation Notes. Enter other information relevant to the investigation.

7. Point of Contact. SSO's name, rank, and telephone number:

(SIGNATURE OF CERTIFYING OFFICIAL)

APPENDIX 3 TO ENCLOSURE 5

CLASSIFICATION REVIEW

Figure 9. Classification Review Format

Date

SUBJECT: Classification Review

THRU: (Appropriate Head of an Element of the IC)

TO: (Requesting SSO)

NOTE: Provide the information below for each document considered compromised. Classify the overall assessment and individual portions thereof according to content.

l. Date of assessment.

2. Name(s) and office symbol(s) conducting assessment.

3. Subject/title, date, number, originator, and original classification of document.

4. May the document be declassified or downgraded, either in whole or in part?

5. Justification for classification:

a. Identify the specific statements in the document that are classified. (This may be done by appending a copy of the document with the classified portions underlined.)

b. Specifically identify the basis for classification, i.e., classified source materials, classified analysis, classification manuals or directives. (This may be done by noting the source materials on the margins of the appended copy of the document.)

c. Provide a complete bibliography of all classified source materials used in the preparation of the document.

6. Are the statements identified above as being classified properly classified?

7. Is the classified information identified above accurate?

8. Has the classified information identified above been the subject of any official release?

9. Did any individual or agency contact your office, as the originator of the material, for authority to release the material in unclassified form?

10. Can the above information identified as classified be edited for the purpose of prosecution or is the subject matter of the information so sensitive that the material should not be considered for use as evidence in a criminal proceeding? (In the revision process, classified material that the Government "cannot live with having revealed in open court" is deleted and replaced with unclassified, generic descriptions of the deleted material. The balance of the document, including classified information that the Government is willing to give up in the interest of obtaining a conviction, is then available for presentation in open court.)

Figure 9. Classification Review Format- Continued

11. May the title of the document be released for trial purpose?

12. May a cleared judge and prosecutor, or possibly defense attorney, examine an unrevised copy of the document in an in camera Classified Information Protection Act (CIPA) hearing incident to a trial? (In a CIPA hearing the defense would be under court order not to reveal classified information and could face a contempt of court citation if classified information is revealed.)

13. Has sufficient background data been published officially or in the press to make an educated speculation on the classified information possible? If so, fully identify the official releases or press reports.

14. Provide the name of the person in your element most competent to testify concerning the classification of the document.

15. Had it been decided to declassify the document prior to the date of compromise, publication, or release of the data?

16. What effect could the disclosure of the classified data in the document have on the national defense?

17. Should any other agencies, activities, or organizations be alerted concerning the compromise or loss of this material?

(SIGNATURE OF VALIDATING OFFICIAL)

ENCLOSURE 6

SECURITY EDUCATION, TRAINING, AND AWARENESS (SETA) PROGRAM

1. SETA. The focal point of any security program should be how well employees understand their responsibilities when it comes to protecting the national security information. To that end, employees at every level must be educated in and frequently reminded of sound security practices and procedures. SETA is the process through which employees are made aware of the threats to, and critical safeguarding procedures of national security information, including SCI. Upon appointment, designated SCI security officials, SSOs, Special Security Representatives, and specified support personnel should attend the DIA Joint Military Intelligence Training Center, SCI Security Officials Course, or similar course within 6 months upon assumption of these duties. SETA is a three-phase program.

a. Phase 1 – Initial indoctrination (security orientation).

b. Phase 2 – Continuing security awareness program (refresher training).

c. Phase 3 – Final awareness instructions (debriefing).

2. PHASE 1 - SECURITY ORIENTATION. A robust SETA program is built on the foundation of the security orientation. This starts with the SCI indoctrination as described in Enclosure 2 of this Volume. Accordingly, employees being indoctrinated into SCI shall receive a security orientation briefing from their local SCI security official. The security orientation briefing shall include, as a minimum:

a. Threat Awareness and Defensive Security Briefing. The local SCI security official, in conjunction with local CI support, shall:

(1) Provide an analysis of the local foreign intelligence and terrorist threat; include insider awareness, technical threats, information assurance, and cyber warfare.

(2) Familiarize employees with their individual protective measures to avoid becoming a target.

(3) Emphasize the importance of contacting the local CI representative, force protection officer, law enforcement agency, and DIA worldwide threat levels for assistance.

b. Overview of the Security Classification Management System. The local SCI, security official in coordination with their classification management expert personnel, shall:

(1) Inform employees about proper classification, marking, and safeguards necessary for accountability and control of classified information.

(2) Notify employees that the improper use of the classification management system is strictly prohibited.

(3) Familiarize employees with the procedures for challenging classification decisions.

(4) Provide employees with the appropriate Executive orders that pertain to classified national security information and agencies that provide guidance (e.g., Information Security Oversight Office, Controlled Access Program Coordination Office).

(5) Inform employees of the requirement to report in advance any marriage to or cohabitation with a foreign national.

c. Explanation of Individual Duties and Responsibilities. The local SCI security official shall:

(1) Provide employees the definition of SCI related terms (e.g., SCIF).

(2) Provide regulatory guidance and local standing operating procedures in the areas of personnel and physical security that shall allow them to operate in a secure SCI environment.

(3) Inform employees of the SCIF's Emergency Action Plan (EAP) and emphasize the importance of their understanding of the emergency destruction or removal guidelines for national security information.

d. Reporting Obligations and Requirements. The local SCI security official shall:

(1) Provide an overview of the requirement to report changes in personal status that may have a bearing on their eligibility for continued access to SCI, as defined in Enclosure 2 of this Volume.

(2) Advise employees that adverse information shall be reported to the local SCI security official expediently, even if the information in question is pending civil decision.

(3) Inform employees of the reporting requirements of any information that raises doubts about the reliability or trustworthiness of co-workers with access to national security information

(4) Inform employees of the outside activities reporting requirements, as defined in Enclosure 2, section 13 of this Volume.

e. Submission for Periodic Reinvestigation. Inform employees of their responsibilities for submitting periodic reinvestigation, as defined in section 11 of Enclosure 2 of this Volume.

f. Prepublication Review Requirement. Advise employees about their responsibility to submit all material for public disclosure to their SCI security official for a prepublication review, as defined in section 15 of Enclosure 2 of this Volume, in addition to any other command requirements for a review by a public affairs official prior to disclosure.

g. IS Security. The local SCI security official in coordination with the Information Assurance Manager or Representative (IAM/R) shall provide an overview of operating procedures of SCI IS security standards and security guidelines for the users. The local SCI security official and the IAM/R shall make employees aware of their basic responsibilities to include, but not limited to:

(1) Protection of physical areas, media, and equipment (e.g., care of media downloading).

(2) Recognition and reporting of security violations on an automated information system.

h. Marking, Handling, and Safeguarding of Classified Material. Provide guidance on the proper marking, safeguarding, and handling of SCI information in their possession, regardless of the media used to obtain the information.

i. Identification of Security POCs. The local SCI security official shall provide employees with the names and telephone numbers of all pertinent security points-of-contact.

j. Local Procedures. Discuss the uniqueness of the supporting SCIF not covered in this enclosure and the information essential to the effectiveness of your organization SETA Program.

k. Derivative Classification Training. Provide training on proper derivative classification procedures as required by Reference (l).

3. PHASE 2 - SETA PROGRAM REFRESHER TRAINING. SETA refresher training is a refresher of Phase 1 and serves as a constant reminder of an employee's duty, obligation, and responsibility to protect classified information. A sound SETA program can prevent unauthorized disclosure and unknown access to our critical information. Local SCI security officials shall provide all indoctrinated employees with security training at least annually. This training shall include, at a minimum, all security training required by Executive Order or DoD policy. Refresher training shall reinforce the training provided during the security orientation and shall keep employees informed of appropriate changes in security regulations and policies. The local SCI security official is encouraged to be as creative as possible in presenting this training. Training methods may include group briefings, videos, dissemination of instructional materials or other media methods. Security awareness training and education shall be formally documented in writing to include the date of the training, the subject(s) covered, the instructor and a method of identifying attendees. The local SCI security official shall retain the record on file for 1 year after the yearly requirement.

4. PHASE 3 - FINAL AWARENESS INSTRUCTIONS (DEBRIEFINGS). When terminating SCI access, emphasize SCI-indoctrinated individual's responsibility to continuously safeguard classified information and address which agencies the individual should report any attempts by unauthorized individuals to solicit national security information.

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ARD	Acquisition Risk Directorate
CAF	central adjudication facility
CI	counterintelligence
CIA	Central Intelligence Agency
CIPA	Classified Information Procedures Act
CM	contract monitor
CO	contracting officer
COMINT	communications intelligence
COMSEC	communications security
COR	contracting officer's representative
CSA	cognizant security authority
CSSO	contractor special security officer
DAC	DIA Counterintelligence and Security Office
DAO	Defense Attaché Office
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DCS	Defense Courier Service
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoDD	DoD directive
DoDI	DoD instruction
DOJ	Department of Justice
DSS	Defense Security Service
DSSCS	Defense Special Security Communications System
EAP	emergency action plan
EO	Executive order
FCL	facility clearance
FFC	fixed facility checklist

FIS	Foreign Intelligence Service
GENSER	general service
GOCO	Government-owned contractor operated
HICE	Head of an Intelligence Community Element
HPSCI	House Permanent Select Committee on Intelligence
HUMINT	human intelligence
IAM	Information Assurance Manager
IAR	Information Assurance Representative
IC	Intelligence Community
ICD	Intelligence Community Directive
ICPG	Intelligence Community Policy Guide
ICS	Intelligence Community Standard
IMA	individual mobilization augmentee
IPA	intergovernmental personnel agreement
ISS	industrial security specialist
JPAS	Joint Personnel Adjudication System (or successor system)
JSO	judicial security officer
JWICS	Joint Worldwide Intelligence Communication System
MOBDES	mobilization designee
NdA	Nondisclosure Agreement
NdS	Nondisclosure Statement
NFIB	National Foreign Intelligence Board
NGA	National Geospatial Intelligence Agency
NRO	National Reconnaissance Office
NFIB	National Foreign Intelligence Board
ORCON	Dissemination and Extraction of Information Controlled by Originator
PCL	personnel security clearance
POC	point of contact

PR	periodic reinvestigation
PROPIN	proprietary information
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SES	Senior Executive Service
SETA	Security Education, Training and Awareness
SF	standard form
SI	special intelligence
SIO	senior intelligence officer
SOIC	senior official to the Intelligence Community
SPA	Special Purpose Access
SSAN	Social Security account number
SSBI	single scope background investigation
SSC	Special Security Center
SSCI	Senate Select Committee on Intelligence
SSN	Social Security number
SSO	special security officer
TK	talent keyhole
TSCM	Technical Surveillance Countermeasures