SUMMARY OF CHANGES TO DoDM 5220.22,
"National Industrial Security Program Operating Manual" (NISPOM)

- Major changes for NISPOM Change 2 are in red font and deletions are lined through in this summary of changes.
- For ease of reference to the user, major changes for NISPOM Change 1, March 28, 2013, are reflected in blue font and deletions are lined through in this summary of changes.
- Cover Page annotated as Incorporating Changes 2, noting date of the change
- Table of Contents has been updated throughout document to reflect current page alignment (Page 2-11)
- References have been updated throughout document to reflect updated or amended guidance (Page 12-14)
- Acronyms added (Pages 15-17)

CHAPTER 1, GENERAL PROVISIONS AND REQUIREMENTS

- Paragraph 1-100: Purpose. This Manual*:*
- Paragraph 1-100a: "*a. ~~i~~I*s issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations *(CFR)*.
- *1-100b. Incorporates and cancels DoD 5220.22-M, Supplement 1 (reference ab).*
- Paragraph 1-101a: "a. The NISP was established by Executive Order (E.O.) 12829 (reference (a)) for the protection of information classified under E.O. ~~12958~~ *13526* (reference (b)) ~~as amended~~, or its successor or predecessor orders, and the Atomic Energy Act of 1954*, as amended* (reference (c))~~, as amended~~…"

- Paragraph 1-101b: "b. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission (NRC) and the Director of ~~*the Central Intelligence Agency (CIA),*~~ *National Intelligence (DNI)* is responsible for the issuance and maintenance of this Manual."

- Paragraph 1-101b(1): "*(1)* The Secretary of Energy and the Chairman of the NRC are responsible for prescribing that portion of the Manual that pertains to information classified under reference (c)*~~, as amended~~. Additionally, the Secretary of Energy and the Chairman of the NRC retain authority over access to information under their respective programs classified under reference (c), and may inspect and monitor contractor, licensee, certificate holder, and grantee programs and facilities that involve access to such information.*

- Paragraph 1-101b(2): "*(2)* The ~~*Director of National Intelligence (*~~DNI~~)~~ is responsible for prescribing that portion of the Manual that pertains to intelligence sources and methods, including SCI. The DNI retains authority over access to intelligence sources and methods, including SCI. *The DNI's responsibilities are derived from the National Security Act of 1947, as amended (reference (d)); Executive Order (EO) 12333, ~~(reference f)~~ as amended (reference (e)); reference (b); and The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (reference (f)). For purposes of this Manual, the DNI* may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information. ~~*The Secretary of Energy and the Chairman of the NRC retain authority over access to information under their respective programs classified under reference (c) as amended. The Secretary or the Chairman may inspect and monitor contractor, licensee, grantee, and certificate holder programs and facilities that involve access to such information.*~~

- Paragraph 1-101e: "e. Nothing in this Manual shall be construed to supersede the authority of the Secretary of Energy or the Chairman of the NRC under reference (c). Nor shall this information detract from the authority of installation commanders under the Internal Security Act of 1950 (reference (~~d~~*g*~~)~~)); ~~*or* the authority of the Director of the Central Intelligence Agency under *the National Security Act of 1947, as amended,* (reference (*e d*)), or E.O. 12333 (reference (*f e*)); as amended by E.O. 13355 (reference (g h))~~; or the authority of the DNI under ~~*the Intelligence Reform and Terrorism Prevention Act of 2004 (*~~reference (~~h~~ f~~)~~). This Manual shall not detract from the authority of other applicable provisions of law, or the authority of any other Federal department or agency head granted according to U.S. statute or Presidential decree.

- Paragraph 1-102c. "Implementation of changes to this Manual by contractors shall be effected no later than 6 months from the date of the published change, *with the exception of changes related to US-UK and US-Australia (AUS) Treaty requirements, in Chapters 4 and 10, Section 8 of this Manual, which must be implemented immediately*."

- Paragraph 1-103b: Adds the Office of Personnel Management: "…(22) the Secretary of Homeland Security; ~~and~~ (23) the Deputy Managing Director, Federal Communications Commission (FCC)*; ~~and~~ (24) the Deputy Director, Facilities, Security, and Contracting, Office of Personnel Management~~–~~; (25) the Archivist, United States National Archives and Records Administration; (26) the President and Chief Executive Officer, Overseas Private Investment Corporation; (27) the Deputy Secretary, Department of Housing and Urban Development; (28) the Chief Executive Officer, Millennium Challenge Corporation; (*29*) the Deputy Assistant to the President and Director, Office of Administration Executive Office of the President; (30) the Associate Commissioner, Office of Security and Emergency Preparedness, Social Security Administration; and (31) the Chief Postal Inspector, United States Postal Service*.

- Paragraph 1-104a: "a. Consistent with paragraph 1-101e, security cognizance remains with each Federal department or agency unless lawfully delegated. The term Cognizant Security Agency (CSA) denotes the Department of Defense (DoD), the Department of Energy (DOE), the NRC, and the ~~Central Intelligence Agency (CIA)~~ *DNI*. The Secretary of Defense, the Secretary of Energy, the ~~Director of the CIA~~ *DNI* and the Chairman, NRC, may delegate any aspect of security administration regarding classified activities and contracts under their purview within the CSA or to another CSA. Responsibility for security administration may be further delegated by a CSA to one or more Cognizant Security Offices (CSO). It is the obligation of each CSA to inform industry of the applicable CSO.

- Paragraph 1-108 added. ***1-108. Releasability and Effective Date***
  a. ***Cleared for public release****. This manual is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.*

  b. Is effective February 28, 2006.

- Chapter 1, Section 2 (Pages 1-2-1 to 1-2-2)
  - Paragraph 1-202 numbering order shifted. ***Insider Threat Program****.*

    a. The contractor will establish and maintain an insider threat program that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, consistent with E.O. 13587 (reference (ac)) and

the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (reference (ad)), as required by the appropriate CSA.

b. The contractor will designate a U.S. citizen employee, who is a senior official and cleared in connection with the FCL, to establish and execute an insider threat program. This Insider Threat Program Senior Official may also serve as the FSO. If the designated senior official is not also the FSO, the contractor's Insider Threat Program Senior Official will assure that the FSO is an integral member of the contractor's implementation program for an insider threat program.

c. *A corporate family may choose to establish a corporate-wide insider threat program with one senior official designated to establish and execute the program. Each cleared legal entity using the corporate-wide Insider Threat Program Senior Official must separately designate that person as the Insider Threat Program Senior Official for that legal entity.*

- Paragraph 1-202 is renumbered and becomes paragraph 1-203. ***1-203.*** **Standard Practice Procedures.**

- Paragraph 1-203 is renumbered and becomes paragraph 1-204. ~~***1-203***~~***1-204*.** **One-Person Facilities.**

- Paragraph 1-204 is renumbered and becomes paragraph 1-205. ~~**1-204**~~***1-205*.** **Cooperation with Federal Agencies and Officially Credentialed Representatives of Those Agencies.** Contractors shall cooperate with Federal agencies and their officially credentialed representatives during official inspections, investigations concerning the protection of classified information and during personnel security investigations of present or former employees and others. Cooperation includes providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours, providing relevant employment and security records *and records pertinent to insider threat (e.g., security, cybersecurity and human resources)* for review when requested, and rendering other necessary assistance.

- Paragraph 1-205 is renumbered and becomes paragraph 1-206. ~~**1-205**~~***1-206*.** **Security Training and Briefings.**

- Paragraph 1-206 is renumbered and becomes paragraph 1-207. ~~**1-206**~~***1-207*.** **Security Reviews**

- Paragraph 1-207b and subparagraphs. "b. **Contractor Reviews.** Contractors shall review their security system on a continuing basis and shall also conduct a formal self-inspection*, including the self-inspection required by paragraph 8-*

101h of chapter 8 of this Manual, at intervals consistent with risk management principles.

(1) These self-inspections will be related to the activity, information, information systems (ISs), and conditions of the overall security program, to include the insider threat program; have sufficient scope, depth, and frequency; and management support in execution and remedy.

(2) The contractor will prepare a formal report describing the self-inspection, its findings, and resolution of issues found. The contractor will retain the formal report for CSA review through the next CSA inspection.

(3) A senior management official at the cleared facility will certify to the CSA, in writing on an annual basis, that a self-inspection has been conducted, that senior management has been briefed on the results, that appropriate corrective action has been taken, and that management fully supports the security program at the cleared facility.

(4) Self-inspections by contractors will include the review of representative samples of the contractor's derivative classification actions, as applicable.

- Paragraph 1-207 is renumbered and becomes paragraph 1-208. ~~**1-207**~~***1-208*.** **Hotlines.** *Federal agencies maintain hotlines to provide an unconstrained avenue for government and contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects. These hotlines do not supplant contractor responsibility to facilitate reporting and timely investigation of security matters concerning its operations or personnel, and contractor personnel are encouraged to furnish information through established company channels. However, the hotline may be used as an alternate means to report this type of information when considered prudent or necessary. Contractors shall inform all employees that the hotlines may be used, if necessary, for reporting matters of national security significance. CSA hotline addresses and telephone numbers are as follows:*

~~CIA Hotline~~
~~Office of the Inspector General~~
~~Central Intelligence Agency~~
~~Washington, D.C. 20505~~
~~(703) 874-2600~~
Defense Hotline
The Pentagon

Washington, DC 20301-1900
(800) 424-9098

U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program, MS 05 E13
11555 Rockville Pike
Rockville, MD 20852-2738
1-800-233-3497
TDD: 1-800-270-2787

DOE Hotline
Department of Energy
Office of the Inspector General
1000 Independence Avenue, S.W. Room ~~5.4235~~ *SD-031*
Washington, D.C. 20585
(202) 586-4073
(800) 541-1625

DNI Hotline
Director of National Intelligence
Office of the Inspector General
Washington, D.C. 20511
(703) 482-2650

- Paragraph 1-208 is renumbered and becomes paragraph 1-208. ~~1-208~~***1-209.*** **Classified Information Procedures Act (CIPA) (Public Law. 96-456, 94 Stat. 2025 codified at Title 18 U.S.C. Appendix 3 (reference (j))).**

- Chapter 1, Section 3 (Pages 1-3-1 to 1-3-2)
  - Paragraph **1-300. General.** Contractors are required to report certain events that*:* ~~have an~~ impact ~~on~~ the status of the facility clearance (FCL)~~,~~*;* ~~that~~ impact ~~on~~ the status of an employee's personnel security clearance (PCL*)* ~~that,~~*; may indicate the employee poses an insider threat;* affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised.

    a. Contractors shall establish such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the FSO, the Federal Bureau of Investigation (FBI), or other Federal authorities as required by this Manual, the terms of a classified contract, and U.S. law. Contractors shall provide complete information to enable the CSA to ascertain whether classified information is

adequately protected. Contractors shall submit reports to the FBI and to their CSA as specified in this section.

~~a~~ *b.* When the reports are classified or offered in confidence and so marked by the contractor, the information will be reviewed by the CSA to determine whether it may be withheld from public disclosure under applicable exemptions of the Freedom of Information Act (5 U.S.C. 552) (reference (k)).

~~b~~ *c.* When the reports are unclassified and contain information pertaining to an individual, the Privacy Act of 1974 (5 U.S.C. 552a)(reference (l)) permits withholding of that information from the individual only to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the U.S. Government under an expressed promise that the identity of the source would be held in confidence. The fact that a report is submitted in confidence must be clearly marked on the report.

- Paragraph 1-302a NOTE: "NOTE: ~~In two court cases, Becker vs. Philco the U.S. Supreme Court upheld the decision in and Taglia vs. Philco (389 U.S. 979), the U.S. Court of Appeals for the 4th Circuit decided on February 6, 1967, that a contractor is not liable for defamation of an employee because of reports made to the Government under the requirements of this Manual and its previous versions.~~ *In Taglia vs. Philco (372 F.2d 771), the U.S. Court of Appeals for the 4th Circuit decided that a contractor is not liable for defamation of an employee because of reports made to the Government under the requirements of this Manual and its previous versions. In Becker v. Philco (389 U.S. 979), the U.S. Supreme Court denied the appeal from the 4th Circuit.*

- Paragraph 1-302j. "**j. Security Equipment Vulnerabilities.** Significant vulnerabilities identified in security equipment, intrusion detection systems (IDS), access control systems, communications security (COMSEC) equipment or systems, and ~~information system (~~IS~~)~~ security hardware and software used to protect classified material."

- Chapter 1, Section 4 (Page 1-4-1). Added new section.

  - Title. ***Section 4. Reports to DoD About Cyber Incidents On Cleared Defense Contractors (CDCs) IS Approved to Process Classified Information***

  - ***1-400. General.***

  a. This section applies only to CDCs.

b. DoD will provide detailed reporting instructions via industrial security letter (ISL) in accordance with DoD Instruction 5220.22 (reference (ae)).

c. This section sets forth the CDC reporting requirements solely for any cyber incidents involving CDC covered ISs that have been approved by the designated DoD NISP CSO to process classified information, referred to in this Manual as a "classified covered IS." A classified covered IS will be considered a type of covered network consistent with the requirements of Section 941 of Public Law 112-239 (reference (af)), and section 391 of Title 10, U.S. code (reference (ag)). The reporting requirements of this section are in addition to the requirements in paragraphs 1-301 or 1-303 of section 3 of this Manual, which can include certain activities occurring on unclassified ISs.

- ***1-401. Reports to be Submitted to DoD.***

a. CDCs will report immediately to DoD any cyber incident on a classified covered IS, as described in paragraph 1-400c of this section.

b. At a minimum, CDCs will report:

(1) A description of the technique or method used in the cyber incident.

(2) A sample of the malicious software, if discovered and isolated by the CDC, involved in the cyber incident.

(3) A summary of information in connection with any DoD program that has been potentially compromised due to the cyber incident.

c. Information that is reported by the CDC (or derived from information reported by the CDC) will be safeguarded, used, and disseminated in a manner consistent with DoD procedures governing the handling of such information reported pursuant to references (af) and (ag) (e.g., as implemented at Part 236 of reference (z) and Subpart 204.73 of Title 48, CFR (reference (ah)), and subject to any additional restrictions based on the classification of the information.

- ***1-402. Access to Equipment and Information by DoD Personnel.***

a. DoD personnel, upon request to the CDC, may be required to obtain access to equipment or information of the CDC that is necessary to conduct forensic analysis in addition to any analysis conducted by the CDC.

b. When access to CDC classified ISs is required, the CDC is only required to provide DoD access to equipment or information, as described in paragraph 1-402a of this section to determine whether information was successfully exfiltrated from a CDC's classified covered IS and if so, what information was exfiltrated.

CHAPTER 2, SECURITY CLEARANCES

- Chapter 2, Section 1 (Pages 2-1-1 to 2-3-2)

  - **2-104. PCLs Required in Connection with the FCL.** The senior management official, ~~and~~ the FSO *and the Insider Threat Program Senior Official* must always be cleared to the level of the FCL. Other officials, as determined by the CSA, must be granted PCLs or be excluded from classified access pursuant to paragraph 2-106.

  - **Paragraph 2-300g**: "g. Nothing contained in this section shall affect the authority of the Head of an Agency to limit, deny or revoke access to classified information under its statutory, regulatory or contract jurisdiction. For purposes of this section, the term "Agency" has the meaning provided at reference (~~i~~*h*), to include the term "DoD Component."

  - **Paragraph 2-303c(2)**. A company that is effectively owned or controlled by a foreign interest may be cleared under an SSA arrangement. Access to proscribed information[~~1~~ *6*] by a company cleared under an SSA may require that the GCA complete a National Interest Determination (NID) to determine that release of proscribed information to the company ~~shall not harm~~*is consistent with* the national security interests of the United States*, in accordance with part 2004 of reference (z)*. The CSA shall advise the GCA on the need for a NID.

    Footnote at the bottom of the page reads: [~~1~~ *6*] Proscribed information includes TS, COMSEC *information or* ~~except classified keys used for data transfer,~~ *material, excluding controlled cryptographic items when unkeyed or utilized with unclassified keys;* RD as defined in reference (c), SAP~~,~~ *information;* ~~, and~~ *or* SCI.

CHAPTER 3, SECURITY TRAINING AND BRIEFINGS

- Chapter 3, Section 1 (Pages 3-1-1 to 3-1-2)

  - **Paragraph 3-102. FSO Training.** Contractors shall be responsible for ensuring that the FSO, and others performing security duties, complete ~~security~~ training considered appropriate by the CSA. Training requirements shall be based on the facility's involvement with classified information and may include an FSO orientation course and for FSOs at facilities with

safeguarding capability, an FSO Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of FSO.

3-103. Insider Threat Training. *The designated Insider Threat Program Senior Official will ensure that contractor program personnel assigned insider threat program responsibilities and all other cleared employees complete training that the CSA considers appropriate.*

a. Contractor insider threat program personnel, including the contractor designated Insider Threat Program Senior Official, must be trained in:

(1) Counterintelligence and security fundamentals, including applicable legal issues.

(2) Procedures for conducting insider threat response actions.

(3) Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.

(4) Applicable legal, civil liberties, and privacy policies.

b. All cleared employees must be provided insider threat awareness training before being granted access to classified information, and annually thereafter. Training will address current and potential threats in the work and personal environment and will include at a minimum:

(1) The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee.

(2) Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within ISs.

(3) Indicators of insider threat behavior, and procedures to report such behavior.

(4) Counterintelligence and security reporting requirements, as applicable.

c. The contractor will establish and maintain a record of all cleared employees who have completed the initial and annual insider threat training. Depending on CSA-specific guidance, a CSA may, instead, conduct such training and retain the records.

- **Paragraph ~~3-103~~ *3-104*. Government-Provided Briefings.** The CSA is responsible for providing initial security briefings to the FSO and for ensuring that other briefings required for special categories of information are provided.

- **Paragraph ~~3-104~~ *3-105*. Temporary Help Suppliers.** A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, shall be responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using contractor may conduct these briefings.

- **Paragraph ~~3-105~~ *3-106*. Classified Information Nondisclosure Agreement (SF 312).** The SF 312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial PCL must execute an SF 312 prior to being granted access to classified information. The contractor shall forward the executed SF 312 to the CSA for retention. If the employee refuses to execute the SF 312, the contractor shall deny the employee access to classified information and submit a report to the CSA. The SF 312 shall be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

- **Paragraph ~~3-106~~ *3-107*. Initial Security Briefings.** Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

  a. A threat awareness *security* briefing*, including insider threat awareness in accordance with paragraph 3-103b of this Manual*.

  b. A ~~*defensive security*~~ *counterintelligence awareness* briefing.

  c. An overview of the security classification system.
  d. Employee reporting obligations and requirements*, including insider threat*.

  e. *Initial and annual refresher cybersecurity awareness training for all authorized IS users (see chapter 8, paragraph 8-101c, of this Manual).*

  f. Security procedures and duties applicable to the employee's job.

- **Paragraph ~~3-107~~ *3-108*. Refresher Training.** The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. *See paragraph 8-103c of chapter 8 of this Manual for the requirement for IS security refresher training.* Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. Contractors shall maintain records about the programs offered and employee participation in them. This requirement may be satisfied by use of distribution lists, facility/department-wide newsletters, or other means acceptable to the FSO.

- **Paragraph ~~3-108~~ *3-109*. Debriefings.** Contractors shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's PCL is terminated, suspended, or revoked; and upon termination of the FCL.

CHAPTER 4, CLASSIFICATION AND MARKING

- Chapter 4, Section 1 (Page 4-1-1)
  - Paragraph 4-101. Original Classification. An original classification decision at any level can be made only by a U.S. Government official who has been *designated or* delegated the authority in writing. A determination to originally classify information may be made only when (a) an original classification authority is classifying the information; (b) the information falls into one or more of the categories set forth in reference (b); (c) the unauthorized disclosure of the information, either by itself or in context with other information, reasonably could be expected to cause damage to the national security, which includes defense against transnational terrorism, that can be identified or described by the original classifier; and (d) the information is owned by, produced by or for, or is under the control of the U. S. Government. The original classifier must state the concise "Reason" for classification on the front of the document. The original classifier must also indicate either a date or event for the duration of classification for up to 10 years from the date of the original classification decision unless the date is further extended due to information sensitivities for up to 25 ~~*or 50*~~ years. *An original classification authority's agency must obtain the approval of the Interagency Security Classification Appeals Panel in order to continue the classification of information beyond 25 years.*

  - Paragraph 4-102. Derivative Classification Responsibilities a. ~~Contractors who extract or summarize classified information, or who apply classification markings derived from a source document, or are directed by a classification guide or a Contract Security Classification Specification, are making derivative classification decisions. The FSO shall ensure that all employees~~

~~authorized to perform derivative classification actions are sufficiently trained and that they possess, or have ready access to, the pertinent classification guides and/or guidance necessary to fulfill these important actions. Any specialized training required to implement these responsibilities will be provided by the CSA upon request.~~ *Contractor personnel make derivative classification decisions when they incorporate, paraphrase, restate, or generate in new form, information that is already classified; then mark the newly developed material consistently with the classification markings that apply to the source information.*

- (New) Paragraph 4-102b: *b. Derivative classification includes the classification of information based on guidance, which may be either a source document or classification guide. The duplication or reproduction of existing classified information is not derivative classification.*

- Paragraph 4-102c: ~~b.~~ c. ~~Employees who copy or extract classified information from another document, or who reproduce or translate an entire document, shall be responsible:~~ *Classified information in e-mail messages is subject to all requirements of reference (b) and Part 2001 of ~~Title 32, CFR, current editions, (~~reference (z)~~).~~ If an e-mail is transmitted on a classified system, includes a classified attachment and contains no classified information within the body of the e-mail itself, then the e-mail is not a derivative classification decision. The e-mail overall classification must reflect the highest level present in the attachment."*

- ~~(1) For marking the new document or copy with the same classification markings as applied to the information or document from which the new document or copy was prepared and~~

- ~~(2) For challenging the classification if there is reason to believe the information is classified unnecessarily or improperly.~~

- Paragraph 4-102d: ~~For information derivatively classified based on multiple sources, the derivative classifier shall: (1) carry forward the date or event for declassification that corresponds to the longest period of classification among the sources, and (2) maintain a listing of those sources on or attached to the official file or record copy.~~ *The contractor shall ensure that all employees authorized to make derivative classification decisions:*

  (1) Are identified by name and position, or by personal identifier, on documents they derivatively classify.

  (2) Observe and respect original classification decisions.

(3) Carry forward the pertinent classification markings to any newly created documents. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(a) The date or event for declassification that corresponds to the longest period of classification among the sources; and

(b) A listing of the source materials.

(4) Are trained, in accordance with CSA direction, in the proper application of the derivative classification principles, with an emphasis on avoiding over-classification, at least once every 2 years. Training will cover classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(5) Are not authorized to conduct derivative classification until they receive such training.

(6) Are given ready access to the pertinent classification guides and/or guidance necessary to fulfill these important actions.

- Paragraph 4-102e: ~~d~~ e ~~Commensurate with their involvement, all personnel who have access to classified information shall be provided with security classification guidance.~~ *Whenever practicable, derivative classifiers shall use a classified addendum if classified information constitutes a small portion of an otherwise unclassified document.*

- Chapter 4, Section 2 (Pages 4-2-1 through Page 4-2-5)
  - Paragraph 4-200. **General.** Physically marking classified information with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified information and material be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, *the identity (by name and position or personal identifier) of the classifier, the source(s) for derivative classification,* and any other notations required for protection of the information.

  - Paragraph 4-202. Identification Markings. All classified material shall be marked to show the name and address of the contractor responsible for its preparation, *the identity of the person (by name and position or personal identifier) responsible*

for each derivative classification action, and the date of preparation. These markings are required on the face of all classified documents.

- Paragraph 4-202. Identification Markings. All classified material shall be marked to show the name and address of the contractor responsible for its preparation, *the identity of the person (by name and position or personal identifier) responsible for each derivative classification action,* and the date of preparation. These markings are required on the face of all classified documents.

- Paragraph **4-206. Portion Markings.**

- Paragraph 4-206. Portion Markings.
a. Each section, part, paragraph, or similar portion of a ~~classified~~ document *containing classified information* shall be marked to show the highest level of its classification *and any applicable control markings*, or ~~that~~ the portion is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contain or reveal classified information. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately ~~following~~ *before* the portion~~'s letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion.~~ *to which it applies. For paragraphs or subparagraphs beginning with numbers, letters or symbols such as bullets, place the portion marking after the number, letter or bullet and before the text.* In marking portions, the parenthetical symbols (TS) for TOP SECRET, (S) for SECRET, (C) for CONFIDENTIAL, and (U) for UNCLASSIFIED shall be used *as well as the authorized abbreviation(s) for any applicable control markings*.

- ~~a.~~*b.* Illustrations, photographs, figures, graphs, drawings, charts, or similar portions contained in classified documents shall be marked clearly to show their classified or unclassified status. These classification markings ~~shall not be abbreviated and~~ shall be prominent and placed within or contiguous to such a portion. Captions of such portions shall be marked on the basis of their content.
- ~~b. If, in an exceptional situation, marking of the portions is determined to be impractical, the classified document shall contain a description sufficient to identify the exact information that is classified and the classification level(s) assigned to it. For example, each portion of a document need not be separately marked if all portions are classified at the same level, provided a full explanation is included in the document.~~

- Paragraph 4-207. Subject and Title Markings. Unclassified subjects and titles shall be selected for classified documents, if possible. A ~~classified~~ subject or title shall be marked with the appropriate symbol placed immediately ~~following~~ *before* the item*, which shall reflect the classification of the title, not the content of the document.*

- Paragraph 4-208. "Markings for Derivatively Classified Documents. All classified information shall be marked to reflect the source of the classification and declassification instructions. Documents shall show the required information either on the cover, first page, title page, or in another prominent position. Other material shall show the required information on the material itself or, if not practical, in related or accompanying documentation.

- *a. CLASSIFIED BY Line. The purpose of the "Classified By" line is to identify the person who applies derivative classification markings for the document. If not otherwise evident, the line will include the* ~~*agency*~~ *contractor and, where available, the office of origin will be identified and follow the name and position or personal identifier of the derivative classifier.*

- *b.* DERIVED FROM" Line. The purpose of the "Derived From" line is to link the derivative classification applied to the material by the contractor and the source document(s) or classification guide(s) under which it was classified. In completing the "Derived From" line, the contractor shall identify the applicable guidance that authorizes the classification of the material. Normally this will be a security classification guide listed on the Contract Security Classification Specification or a source document. When identifying a classification guide on the "Derived From" line, the guide's title or number, issuing agency, and date shall be included. Many Contract Security Classification Specifications cite more than one classification guide and/or the contractor is extracting information from more than one classified source document. In these cases, the contractor may use the phrase "multiple sources." When the phrase "multiple sources" is used, the contractor shall ~~maintain records that support the classification for the duration of the contract under which the material was created. These records~~ *include a listing of the source materials in, or attached to, each derivatively classified document. This listing* may take the form of a bibliography identifying the applicable classification sources. ~~and be included in the text of the document or they may be maintained with the file or record copy of the document. When practical, this information should be included in or with all copies of the derivatively classified document. If the only source for the derivative classification instructions is the Contract Security Classification Specification, the date of the specification and the specific contract number for which it was issued shall be included on the "Derived From" line.~~

- ~~b.~~ *c.* "DECLASSIFY ON" Line. The purpose of the "Declassify On" line is to provide declassification instructions appropriate for the material. When completing this line, the contractor shall use the information specified in the Contract Security Classification Specification or classification guide furnished with a classified contract. Or, the contractor shall carry forward the duration instruction from the source document or classification guide (e.g., date or event).

When the source is marked "Original Agency's Determination Required" (OADR), ~~or~~ "X1 through X8", *Manual Review (MR), "DNI Only," "DCI Only," or contains any other no longer valid declassification instruction,* the "Declassify On" line ~~should indicate that the source material was marked~~ *shall be marked* with ~~one of these instructions and the date of origin of the most recent source document as appropriate to the circumstances.~~ *a date that is 25 years from the date of the source document, unless other guidance has been provided by the OCA.* When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the "Declassify On" line shall reflect the longest duration of any of its sources. Material containing RD or FRD shall not have a "Declassify On" line *unless co-mingled with national security information subject to reference (b).*

- ~~c.~~ *d.* "DOWNGRADE TO" Line. When downgrading instructions are contained in the Contract Security Classification Specification, classification guide or source document a "Downgrade To" line will be included. When completing this line, the contractor shall insert SECRET or CONFIDENTIAL and an effective date or event. The markings used to show this information are:

  DERIVED FROM
  DOWNGRADE TO ON
  DECLASSIFY ON

- ~~d.~~ *e.* ~~**"CLASSIFIED BY" Line and**~~ **"REASON CLASSIFIED" Line**. As a general rule, ~~a "Classified By" line and~~ a "Reason Classified" line will be shown only on originally classified documents. However, certain agencies may require that derivatively classified documents contain a ~~"Classified By"line to identify the derivative classifier and a~~ "Reason Classified" Line to identify the specific reason for the derivative classification. Instructions for the use of these lines will be included in the security classification guidance provided with the contract.

- ~~e. **"REASON CLASSIFIED" Line**. As a general rule, a "Reason Classified" line will be shown only on originally classified documents. However, certain agencies may require that derivatively classified documents contain a "Reason Classified" Line to identify the specific reason for the derivative classification. Instructions for the use of these lines will be included in the security classification guidance provided with the contract.~~

- Paragraph 4-210b: b. E-mail and other Electronic Messages. Electronically transmitted messages shall be marked in the same manner required for other documents except as noted. The overall classification of the message shall be the first item of information in the text *and shall be displayed at the top and bottom of each message*. A *"Classified By" line, a* "Derived From" line, a "Declassify On"

line, is *and portion markings are* required on messages. Certain agencies may also require that messages contain a ~~"Classified By" and a~~ "Reason Classified" line in order to identify the ~~derivative classifier and the~~ specific reason for classification, *which is carried over from the source document(s) or classification guide.* Instructions for the use of such lines will be included in the security classification guidance provided with the contract documents. *E-mail transmitted on or prepared for transmission on classified systems or networks shall be configured to display:*

- Paragraph 4-210b: b. E-mail and other Electronic Messages. Electronically transmitted messages shall be marked in the same manner required for other documents except as noted. The overall classification of the message shall be the first item of information in the text and shall be displayed at the top and bottom of each message. A "Classified By" line, a "Derived From" line, a "Declassify On" line, ~~is~~ and portion markings are required on messages. ~~Certain agencies may also require that messages contain a "Reason Classified" line in order to identify the specific reason for classification, which is carried over from the source document(s) or classification guide. Instructions for the use of such lines will be included in the security classification guidance provided with the contract documents.~~ E-mail transmitted on or prepared for transmission on classified systems or networks shall be configured to display:

- *(1) The overall classification at the top and bottom of the body of each message; the overall classification marking string for the e-mail will reflect the classification of the header and body of the message, including the subject line, the text of the e-mail, a classified signature block, attachments, included messages, and any other information conveyed in the body of the e-mail; classified e-mail will be portion marked.*

- *(2) When forwarding or replying to an e-mail, contractors shall ensure that the classification markings reflect the overall classification and declassification instructions for the entire string of e-mails and attachments. This includes any newly drafted material, material received from previous senders, and any attachments.*

- *(3)* When messages are printed by an automated system, all markings may be applied by that system, provided the classification markings are clearly distinguished from the printed text. *The markings required by paragraph 4-208 shall be included after the signature block, but before the overall classification marking at the end of the e-mail.* The last line of ~~*text of*~~ the message shall ~~include the declassification instructions~~ *be the overall classification of the e-mail*.

- Paragraph **4-211. Marking Transmittal Documents.** A transmittal document shall be marked with the highest level of classified information *and applicable control markings, if any,* contained in the document and with an appropriate notation to indicate its classification when the enclosures are removed. An unclassified document that transmits a classified document as an attachment shall bear a notation substantially as follows: "Unclassified when Separated from Classified Enclosures." A classified transmittal that transmits higher classified information shall be marked with a notation substantially as follows: "CONFIDENTIAL (or SECRET) when Separated from Enclosures." In addition, a classified transmittal itself must bear all the classification markings required for a classified document.

- Paragraph 4-213. Marking Compilations**.** In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. *The determination that information requires classification by compilation will be based on specific guidance regarding compilation provided in a Contract Security Classification Specification or a security classification guide. If specific guidance is absent, the contractor will obtain written guidance from the applicable GCA.* When classification is required to protect a compilation of such information, the overall classification assigned to the compilation shall be conspicuously affixed. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the compilation. ~~In this instance, the portions of a compilation classified in this manner need not be marked.~~ *Any unclassified portions will be portion marked (U), while the overall markings will reflect the classification of the compiled information, even if all the portions are marked (U).*

- (New) *Paragraph 4-214. **Working Papers.** Working papers containing classified information shall be dated when created; marked with the highest classification of any information contained in them; protected at that level; and if otherwise appropriate, destroyed when no longer needed. Working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level if released outside of the facility, filed permanently, or retained for more than 180 days from the date of the origin, filed permanently, e-mailed within or released outside the originating activity.*

- ~~**4-214**~~ ***4-215.*** Marking Miscellaneous Material. Material developed in connection with the handling, processing, production, *storage* and utilization of classified information shall be handled in a manner that ensures adequate protection of the classified information involved and shall be destroyed at the earliest practical time, unless a requirement exists to retain such material. There is no requirement to mark such material.

- PARAGRAPH NUMBER CHANGED: ~~**4-215**~~ ***4-216.*** Marking Training Material.

- PARAGRAPH NUMBER CHANGED: ~~**4-216**~~ ***4-217*****.** Downgrading or Declassification Actions.

- PARAGRAPH NUMBER CHANGED: ~~**4-217**~~ ***4-218*****.** Upgrading Action

- PARAGRAPH NUMBER CHANGED: ~~**4-218**~~ ***4-219*****.** Inadvertent Release.

- **NEW:** ***Paragraph 4-220.*** *Marking requirements for transfers of defense articles to AUS or the United Kingdom (UK). Marking requirements for transfers of defense articles to AUS or ~~the United Kingdom~~ UK without a license or other written authorization are located in Chapter 10, Section 8 of this Manual.*

- **NEW:** ***Paragraph* 4-221. *Comingling of Restricted Data and Formerly Restricted Data.*** *To the greatest degree possible, do not comingle RD and FRD in the same document with information classified pursuant to reference (b). When mixing can't be avoided, the requirements of references (b) and (x) must be met.*

CHAPTER 5, SAFEGUARDING CLASSIFIED INFORMATION

- Chapter 5, Section 2 (Page 5-2-1)

  - Paragraph 5-203a: a. A record of TOP SECRET material produced by the contractor shall be made when the material is: (1) completed as a finished document, (2) retained for more than ~~30~~ 180 days after creation, regardless of the stage of development, or (3) transmitted outside the facility.

  - Paragraph 5.203b: b. Classified working papers generated by the contractor in the preparation of a finished document shall be: (1) dated when created, (2) marked with its overall classification and with the annotation "WORKING PAPERS", and (3) destroyed when no longer needed. Working papers shall be marked in the same manner prescribed for a finished document at the same classification level *if* ~~when: (1) transmitted~~ *released* outside the facility, or ~~(2)~~ retained for more than ~~30 days from creation for TOP SECRET, or~~ 180 days from ~~*creation for SECRET and CONFIDENTIAL material.*~~ *the date of origin.*

- Chapter 5, Section 3 (Pages 5-3-1 to 5-3-2)

  - **5-300. General**. This section describes the uniform requirements for the physical protection of classified material in the custody of contractors. Where these requirements are not appropriate for protecting specific types or forms of classified material, compensatory provisions shall be developed and approved by the CSA. Nothing in this ~~*m*~~*M*anual shall be construed to contradict or inhibit compliance with the law or building codes. Cognizant security officials shall work to meet appropriate security needs according to the intent of this ~~*m*~~*M*anual and at acceptable cost.

- **5-303. SECRET Storage.** SECRET material shall be stored in a GSA-approved security container, an approved vault, or closed area. Supplemental controls are required for storage in closed areas. ~~The following additional storage methods may be used until October 1, 2012:~~

  ~~a. A safe, steel file cabinet, or safe-type steel file container that has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours.~~

  ~~b. Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar shall be secured to the cabinet by welding, rivets, or bolts so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely so their contents cannot be removed without forcing open the drawer. This type of cabinet will be accorded supplemental protection during non-working hours.~~

- Paragraph **5-311. Repair of Approved Containers.** Repairs, maintenance, or other actions that affect the physical integrity of a security container approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers. Repair procedures may be obtained from the CSA.

  a. An approved security container is considered to have been restored to its original state of security integrity if all damaged or altered parts are replaced with manufacturer's replacement or identical cannibalized parts. ~~A signed and dated certification for each repaired container, provided by the repairer, shall be on file setting forth the method of repair used.~~

  b. ~~A container repaired using other than approved methods may be used for storage of SECRET material with supplemental controls only until October 1, 2012~~*The repairer will provide a signed and dated certification for each repaired container that describes the method of repair used; certifications will be kept on file by the contractor*.

- Chapter 5, Section 8 (Page 5-8-1)

  - Paragraph 5-800, Page: 5-8-1: This section describes the construction requirements for closed areas and vaults. Construction shall conform to the requirements of this section or, with CSA approval, to the standards of ~~DCID 6/9~~

Intelligence Community *(IC)* Directive 705, "Sensitive Compartmented Information Facilities (SCIFs) (reference (~~o~~n)).

CHAPTER 6, VISITS AND MEETINGS

- Chapter 6, Section 1 (Page 6-1-1)

  - Paragraph **6-105. Long-Term Visitors**

    b. Government personnel assigned to or visiting a contractor facility and engaged in oversight of an acquisition program shall retain control of their work product. Classified work products of government employees shall be handled in accordance with this ~~m~~*M*anual. Contractor procedures shall not require government employees to relinquish control of their work products, whether classified or not, to a contractor

- Chapter 6, Section 2 (Page 6-2-1)

  - Paragraph **6-201a(7)**. A description of the security arrangements necessary for the meeting to comply with the requirements of this ~~m~~*M*anual.

CHAPTER 7, SUBCONTRACTING

- Chapter 7, Section 1 (Page 7-1-1)

  - Paragraph 7-101b(2). If a prospective subcontractor does not have the appropriate FCL or safeguarding capability, the prime contractor shall request the CSA of the subcontractor to initiate the necessary action. Requests shall include, as a minimum, the full name, address and contact information for the requester; the full name, address, and contact information for a contact at the facility to be processed for an FCL; the level of clearance and/or safeguarding capability required; and full justification for the request. Requests for safeguarding capability shall include a description, quantity, end-item, and classification of the information related to the proposed subcontract. Other factors necessary to help the CSA determine if the prospective subcontractor meets the requirements of this ~~m~~*M*anual shall be identified, such as any special access requirements.

CHAPTER 8, ~~INFORMATION SYSTEM~~ *IS* SECURITY

- Chapter 8, Section 1 (Page 8-1-1)

- Paragraph **8-100. General**

  a. ~~Information systems (IS)~~ *Contractor ISs* that are used to capture, create, store, process or distribute classified information must be properly managed to protect

against unauthorized disclosure of classified information. *Protection concerning* loss of ~~*data integrity to ensure* the~~ availability *or integrity* of the ~~data~~ *information* ~~and~~ *on the* system *must be established separately by contract*. *ISs security will use a risk-based approach, including a baseline set of management, operational, and technical controls.*

b. Protection requires a balanced approach including IS*s* security features to include but not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the IS*s* are required.

c. ~~The requirements outlined in the following sections apply to all information systems processing classified information. Additional requirements for high-risk systems and data are covered in the NISPOM Supplement~~ *Banners will be included on all classified ISs to notify users they are subject to monitoring and that such monitoring could be used against them in a criminal, security, or administrative proceeding.*

d. The contractor will implement protection measures in accordance with guidance issued by the CSA, including tools or capabilities required by the CSA to monitor user activity on classified ISs in order to detect activity indicative of insider threat behavior. The guidance the CSA issues will be based on requirements for Federal systems, as established by section 3541, et seq. of title 44, U.S.C., also known as the "Federal Information Security Management Act" (reference (ai)) and defined in National Institute of Standards and Technology Special Publication (NIST) 800-37 (reference (aj)), Committee on National Security Systems (CNSS) Directive 504 (reference (ak)), and other applicable CNSS publications (e.g., NIST Special Publication 800-53 (reference (al)) and CNNSI No. 1253 (reference (am)). The CSA may provide profiles containing security controls appropriate for specific types of systems, configurations, and environments.

e. The requirements outlined in the following sections apply to all ISs processing classified information. Additional requirements for high-risk systems and data are covered in Appendix D of this Manual.

- ~~Paragraph **8-101. Responsibilities**~~***ISs Security Program.*** *The contractor will maintain an ISs security program that incorporates a risk-based set of management, operational and technical controls, consistent with guidelines established by the CSA. The ISs security program must include, at a minimum, the following elements:*

a. ~~The CSA shall establish a line of authority for training, oversight, program review, certification, and accreditation of IS used by contractors for the processing of classified information. The CSA will conduct a risk management evaluation based on~~

~~the contractor's facility, the classification, and sensitivity of the information processed. The evaluation must ensure that a balanced, cost-effective application of security disciplines and technologies is developed and maintained.~~ *Policies and procedures that reduce information security risks to an acceptable level and address information security throughout the IS life cycle.*

b. ~~Contractor management will publish and promulgate an IS Security Policy addressing the classified processing environment. Additionally, an IS Security Manager (ISSM) will be appointed with oversight responsibility for the development, implementation, and evaluation of the facility's IS security program. Contractor management will assure that the ISSM is trained to a level commensurate with the complexity of the facility's IS.~~ *Plans for providing adequate information security for data resident in the IS or on the networks, facilities, or groups of ISs, as appropriate.*

c. In addition to the training requirements outlined in paragraphs 3-107 and 3-108 of chapter 3 of this Manual, all IS authorized users will receive training on the security risks associated with their user activities and responsibilities under the NISP. The contractor will determine the appropriate content of the security training taking into consideration, assigned roles and responsibilities, specific security requirements, and the ISs to which personnel are authorized access.

d. Testing and evaluation of information security policies, procedures, practices, and security control implementation no less than annually to reflect a continuous monitoring approach of IS related risk assumptions and security control effectiveness.

e. A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices.

f. Procedures for detecting, reporting, and responding to security incidents and events.
g. Plans and procedures for ISs continuity of operations when required by contract.

h. A self-inspection program in accordance with paragraph 1-207b of chapter 1 of this Manual.

- ~~Paragraph **8-102. Designated Accrediting/Approving Authority**~~ ***System Security Plan (SSP)*****.** ~~The CSA is the Designated Accrediting/Approving Authority (DAA) responsible for accrediting information systems used to process classified information in industry~~ *The contractor will document ISs protections in the SSP. The SSP provides a summary of the security requirements for the ISs and describes the security controls in place. The SSP may reference other key security-related documents for the ISs, e.g., a risk assessment, plan of action and milestones, authorization decision letter, contingency plan,*

configuration management plan, security configuration checklist, and system interconnection agreement, as appropriate.

- ~~Paragraph **8-103. IS Security Manager (ISSM)**~~***Contractor Responsibilities*****.** ~~The ISSM:~~ *The contractor will certify to the CSA that the ISs to be used for processing classified information includes an ISs security program that addresses the management, operational, and technical controls in accordance with CSA-provided guidelines. Contractors that are, or will be, processing classified information on an IS must appoint an employee to serve as the ISs Security Manager (ISSM). It is the responsibility of the contractor to assure that the ISSM is adequately trained and possesses technical competence commensurate with the complexity of the contractor's ISs.*

  a. ~~Ensures the development, documentation, and presentation of IS security education, awareness, and training activities for facility management, IS personnel, users, and others, as appropriate.~~ *The ISSM will:*

    (1) Oversee the development, implementation, and evaluation of the contractor's ISs program, including insider threat awareness, for facility management, ISs personnel, users, and others, as appropriate. The ISSM must coordinate with the contractor's FSO and the contractor's Insider Threat Program Senior Official to ensure insider threat awareness is addressed within the contractor's ISs program.

    (2) Possess sufficient experience, command adequate resources, and be organizationally aligned to ensure prompt support and successful execution of a robust ISs security program.

    (3) Develop, document, and monitor compliance with and reporting of the contractor facility's ISs security program in accordance with CSA-provided guidelines for management, operational, and technical controls.

    (4) Verify self-inspections are conducted on the contractor's ISs and corrective actions are taken for all identified findings and vulnerabilities.

    (5) Certify to the CSA, in writing, each SSP has been implemented; the specified security controls are in place and properly tested; and the IS continues to function as described in the SSP.

    (6) Brief users on their responsibilities with regard to ISs security and verify contractor personnel are trained on the ISs prescribed security restrictions and safeguards before they are allowed to access a system.

  b. ~~Establishes, documents, implements, and monitors the IS Security Program and related procedures for the facility and ensures facility compliance with requirements for IS.~~ *The ISSM may assign an IS Security Officer (ISSO). If assigned, the ISSO will:*

(1) Verify the implementation of delegated aspects of the contractor's ISs Security Program from the ISSM and security measures, in accordance with CSA and contractor procedures.

(2) Conduct self-inspections and provide corrective actions to the ISSM.

c. ~~Identifies and documents unique local threats/vulnerabilities to IS.~~ *All IS users will:*

(1) Comply with the ISs security program requirements as part of their responsibilities for the protection of ISs and classified information.

(2) Be accountable for their actions on an IS.

(3) Not share any authentication mechanisms (including passwords) issued for the control of their access to an IS.

(4) Protect authentication mechanisms at the highest classification level and most restrictive classification category of information to which the mechanisms permit access.

(5) Be subject to monitoring of their activity on any classified network and the results of such monitoring could be used against them in a criminal, security, or administrative proceeding.

~~d. Coordinates the facility IS Security Program with other facility security programs.~~

~~e. Ensures that periodic self-inspections of the facility's IS Program are conducted as part of the overall facility self-inspection program and that corrective action is taken for all identified findings and vulnerabilities. Self-inspections are to ensure that the IS is operating as accredited and that accreditation conditions have not changed.~~

~~f. Ensures the development of facility procedures to:~~

~~(1) Govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.~~

~~(2) Properly implement vendor supplied authentication (password, account names) features or security-relevant features.~~

~~(3) Report IS security incidents to the CSA. Ensure proper protection or corrective measures have been taken when an incident/vulnerability has been discovered.~~

(4) Require that each IS user sign an acknowledgment of responsibility for the security of the IS.

(5) Implement security features for the detection of malicious code, viruses, and intruders (hackers), as appropriate.

g. Certifies to the CSA, in writing, that each System Security Plan (SSP) has been implemented; that the specified security controls are in place and properly tested; and that the IS is functioning as described in the SSP.

h. Ensures notification of the CSA when an IS no longer processes classified information, or when changes occur that might affect accreditation.

i. Ensures that personnel are trained on the IS's prescribed security restrictions and safeguards before they are initially allowed to access a system.

j. Develops and implements general and remote maintenance procedures based on requirements provided by the CSA.

- Paragraph **8-104. Information System Security Officer(s) (ISSO).** ISSOs may be appointed by the ISSM in facilities with multiple accredited IS. The ISSM will determine the responsibilities to be assigned to the ISSO that may include the following:

a. Ensure the implementation of security measures, in accordance with facility procedures.

b. Identify and document any unique threats.

c. If so directed by the GCA and/or if an identified unique local threat exists, perform a risk assessment to determine if additional countermeasures beyond those identified in this chapter are required.

d. Develop and implement a certification test as required by the ISSM/CSA.

e. Prepare, maintain, and implement an SSP that accurately reflects the installation and security provisions.

f. Notify the CSA (through the ISSM) when an IS no longer processes classified information, or when changes occur that might affect accreditation.

g. Ensure:

(1) That each IS is covered by the facility Configuration Management Program, as applicable.

(2) That the sensitivity level of the information is determined prior to use on the IS and that the proper security measures are implemented to protect this information.

(3) That unauthorized personnel are not granted use of, or access to, an IS.

(4) That system recovery processes are monitored to ensure that security features and procedures are properly restored.

h. Document any special security requirement identified by the GCA and the protection measures implemented to fulfill these requirements for the information contained in the IS.

i. Implement facility procedures:

(1) To govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.

(2) To ensure that vendor-supplied authentication (password, account names) features or security-relevant features are properly implemented.

(3) For the reporting of IS security incidents and initiating, with the approval of the ISSM, protective or corrective measures when a security incident or vulnerability is discovered.

(4) Requiring that each IS user sign an acknowledgment of responsibility for the security of IS and classified information.
(5) For implementing and maintaining security-related software for the detection of malicious code, viruses, and intruders (hackers), as appropriate.

j. Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.

k. Evaluate proposed changes or additions to the IS, and advises the ISSM of their security relevance.

l. Ensure that all active user Ids are revalidated at least annually.

- Paragraph **8-105. Users of IS.** Users of IS are either privileged or general users.

a. Privileged users have access to IS control, monitoring or administration functions. Examples include:

~~(1) Users having "superuser," "root," or equivalent access to a system (e.g., system administrators, computer operators, ISSOs); users with near or complete control of an IS or who set up and administer user accounts and authenticators.~~

~~(2) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexers, and other key IS equipment.~~

~~(3) Users who have been given the authority to control and change other users' access to data or program files (e.g., applications software administrators, administrators of specialty file systems, database managers).~~

~~(4) Users who have been given special access for troubleshooting or monitoring an IS' security functions (e.g., those using analyzers, management tools).~~

~~b. General users are individuals who can input information to or modify information on an IS or who can receive information from an IS without a reliable human review.~~

~~c. All users shall:~~

~~(1) Comply with the IS Security Program requirements.~~

~~(2) Be aware of and knowledgeable about their responsibilities in regard to IS security.~~

~~(3) Be accountable for their actions on an IS.~~

~~(4) Ensure that any authentication mechanisms (including passwords) issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.~~

~~(5) Acknowledge, in writing, their responsibilities for the protection of the IS and classified information.~~

- Section 2. ~~Certification and Accreditation~~*Assessment and Authorization* (Page 8-2-1)

  - Paragraph **8-200. Overview.** ~~The certification and accreditation (C&A) process~~ is ~~an~~ integral ~~part of the life cycle of an IS~~. ~~The identification of protection measures occurs during system design or development. The formal C&A occurs after the protection measures have been implemented and any required IS protection documentation has been approved. Certification validates that the protection measures described in the SSP have been implemented on the system and that the protection measures are functioning properly. Accreditation is the approval by the CSA for the system to process classified information.~~ *Assessment and*

authorization of classified networks and ISs is integral to managing information security-related risks. Execution of these tasks helps to ensure security capabilities provided by the selected security controls are implemented, tested, validated, and approved by the authorizing official (AO), designated by the applicable CSA, with a degree of assurance appropriate for their information protection needs.

- Paragraph **8-201.** ~~**Certification Process**~~ ***Assessment*****.** ~~Certification is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. The certification process subjects the system to appropriate verification that protection measures have been correctly implemented.~~ *Security control assessment is a combined effort by the contractor and the CSA.* The ~~ISSM shall~~ *contractor will* review*,* ~~and~~ certify*, and attest* to the CSA that all systems have the appropriate protection measures in place ~~and validate that they provide the protection intended~~. The CSA ~~may conduct an onsite assessment to validate the ISSM's review and certification of the IS~~ *must receive the most complete, accurate, and trustworthy information to make timely, credible, and risk assessment based decisions on whether to authorize ISs operation*.

- Paragraph **8-202.** ~~**Accreditation**~~ ***Authorization*****.** ~~The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.~~ *The AO, on behalf of the U.S. Government, will render an operational authorization decision based on the results of security assessment activities and the implementation of the CSA-provided set of security controls. All ISs must be authorized before processing classified information. The AO may choose to eliminate the authorization termination date (ATD) if the contractor's continuous monitoring program is sufficiently robust to provide the AO with needed information with regard to the security state of the ISs and the ongoing effectiveness of security controls in accordance with reference (al) and the Office of Management and Budget Memorandum M-14-03 (reference (an)) or their successors.*

  a. **Interim** ~~**Approval**~~ ***Authorization*** **to Operate** ***(IATO)*****.** The ~~CSA~~ *AO* may grant interim ~~approval~~ *authorization* (temporary authority) ~~to operate an IS~~ *for an initial period*~~. Interim approval to operate may be granted for~~ up to 180 days with an option for the ~~CSA~~ *AO* to extend the interim approval for an additional 180 days. *The contractor will have the* CSA-approved protection measures ~~shall be~~

~~(management, operational and technical security controls)~~ in place and functioning during the period of ~~interim approval~~ *the IATO*.

b. ~~**Reaccreditation**~~ ***ATO*.** ~~IS shall be reaccredited whenever security relevant changes are made to the accredited IS. Proposed modifications to an IS shall be reviewed by the ISSM to determine if the proposed modifications will impact the protections on the system. If the protection aspects of the system's environment change, if the applicable IS protection requirements change, or if the protection mechanisms implemented for the system change, the system shall be reaccredited. During the reaccreditation cycle, the CSA may grant an interim approval to operate the system.~~ *The AO may grant an authorization to operate (ATO) following validation of the CSA-approved protection measures conducted during the IATO period, or may grant an ATO without an IATO period.*

c. ~~**Review of Security-Relevant Changes.** All modifications to security-relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved in accordance with procedures prior to implementation. All security-relevant changes shall be subject to the provisions of the system configuration management program. The ISSM shall notify the CSA of requests for changes to the resources that deviate from the requirements of the approved SSP. The CSA shall determine if system reaccreditation is required.~~

~~d. **Re-evaluation of an Accreditation.** Each IS shall be re-evaluated for reaccreditation every 3 years. Such review involves a determination by the CSA, with input from the ISSM that the conditions under which the original accreditation was granted still apply. If the accreditation remains valid, the accreditation originally furnished by the CSA need only be annotated that the re-evaluation was conducted and the date of the re-evaluation.~~

~~e. **Withdrawal of Accreditation.** The CSA shall evaluate the risks and consider withdrawal of accreditation if the protection measures approved for the system do not remain effective or whenever any of the following items change: levels of concern, protection level, technical or nontechnical protection measures, vulnerabilities, operational environment, operational concept, or interconnections. The CSA shall withdraw accreditation and ensure proper sanitization when the system is no longer required to process classified information, or if the operational need for the system no longer outweighs the risk of operating the system.~~

~~f. **Invalidation of an Accreditation.** The CSA will be notified and an accreditation will become invalid immediately whenever detrimental, security-significant changes occur to any of the following: the required protection level; the operational environment; or the interconnections.~~

~~g. **Certification and Accreditation of Similar Systems.** If two or more similar IS are to be operated in equivalent operational environments (e.g., the levels of concern and protection level are the same, the users have at least the required clearances and access approvals for all information on the IS, the IS configurations are essentially the same, and the physical security requirements are similar), a Master SSP may be written by the ISSO, certified by the ISSM, and then approved by the CSA to cover all such IS. The IS covered by a Master SSP may range from stand alone workstations up to and including multi-user IS and local networks that meet the criteria for a Master SSP approach. This type of approval applies only to systems operating at Protection Levels 1 and 2 (see 8-402).~~

c. ***Security-Relevant Changes.*** *All modifications to security-relevant resources of an authorized IS (including software, firmware, hardware, or interfaces and interconnections to networks) must be approved in accordance with CSA-provided guidelines before implementation. The CSA will review all security-relevant changes based on provisions of the system configuration management program and CSA guidelines. The contractor will notify the CSA of all changes that deviate from the requirements of the approved SSP. The CSA will then notify the contractor if system reauthorization is required. During the reauthorization process, the CSA may grant an IATO.*

(1) ~~Master Information Systems Security Plan. The Master SSP shall specify the information required for each certification for an IS to be accredited under the plan.~~ *Examples of security-relevant changes to an IS that should be reviewed for possible reauthorization include, but are not limited to:*

(a) Installation of a new or upgraded operating system, middleware component, or application;

(b) Modifications to networks, nodes, system ports, protocols, or services;

(c) Installation of a new or upgraded hardware platform or firmware component; or

(d) Modifications to cryptographic modules or services.

(2) ~~An IS Certification Report shall contain the information system identification and location and a statement signed by the ISSM certifying that the IS implements the requirements in the Master SSP.~~ *Changes in laws, directives, policies, or regulations, while not always directly related to the IS, can potentially affect the security of the system and trigger a reauthorization action.*

(3) ~~The CSA shall accredit the first IS under the Master SSP. All other IS to be operated under the Master SSP shall be certified by the ISSM as meeting the conditions of the approved Master SSP. This certification, in effect, accredits the individual IS to operate under the Master SSP. A copy of each certification report shall be retained with the approved copy of the Master SSP.~~ *Applying security patches and performing other maintenance actions that do not affect the protection features of the IS, as previously validated by the CSA, are not considered security relevant changes and therefore do not require the reauthorization of an IS.*

d. ***Re-evaluation of an Authorization****. Each IS will be reevaluated for authorization every 3 years, or at shorter intervals if required by the CSA. The reevaluation of an authorization by a CSA involves input from the ISSM that the conditions under which the original authorization was granted still apply. CSA-provided guidance will include procedures and record-keeping requirements for reevaluation of an authorization as follows:*

(1) The IS has no ATD or no security relevant changes.

(2) The IS has an ATD, or has security relevant changes.

~~(4) Recertification. IS certified under a Master SSP remain certified until the Master SSP is changed or 3 years have elapsed since the IS was certified. If either the levels of concern or protection level described in the Master SSP change, the Master SSP shall be re-accredited by the CSA and all IS certified under the Master SSP shall be re-certified by the ISSM in coordination with the CSA.~~

~~h. **Systems under Multiple CSAs.** For a system that involves multiple CSAs, the CSAs shall designate a primary CSA. Each facility involved in the system shall identify, in writing, the security officials who are responsible for implementing IS protection on the system components at their respective facility.~~

e. Withdrawal of Authorization*. The CSA will evaluate the risks and consider withdrawal of authorization if the management, operational or technical protection measures approved for the system do not remain effective, or if classified information is placed at risk. The CSA may withdraw authorization at any time based on those considerations. The contractor will sanitize or destroy classified media via approved government procedures when the IS is no longer required to process classified information unless retention has been authorized in accordance with a final contract security classification specification. The method of sanitization or destruction of classified media must be accomplished using CSA guidance before action is taken. Audit logs will be retained for 12 months or until the next inspection.*

f. Invalidation of an Authorization*. The contractor will notify the applicable CSA personnel (e.g., the AO), whenever detrimental, security-relevant changes occur to any of the following: the required protection level, the operational environment, the interconnections, or as specified in CSA guidelines. If the CSA determines classified information is at risk, the CSA will notify the contractor and the authorization of the IS will become invalid immediately. If the contractor determines classified information on the IS is at risk, the contractor will cease processing classified information on the affected IS and notify the CSA immediately.*

- Section 3. ~~**Common Requirements**~~***Security Controls*** (Pages 8-3-1 to 8-3-3)

  - Paragraph **8-300.** ~~**Introduction**~~***Security Controls*****.** This section describes the ~~protection requirements that are common to all IS~~*minimum parameters for management, operational, and technical controls that contractors are required to implement. Additional security controls may be provided by the CSA to establish the baseline security control set required for each IS processing classified information.*

  - Paragraph **8-301.** ~~**Clearing and Sanitization.** Instructions on clearing, sanitization and release of IS media shall be issued by the accrediting CSA.~~ ***Management Controls.*** *Contractors will apply the following control measures:*

    a. ~~**Clearing**~~ ***System and Services Acquisition*** ~~Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.~~

    (1) Allocate sufficient resources to adequately protect ISs.

    (2) Employ system development cycle processes that address information security considerations.

    (3) Employ software usage and installation restrictions.

    b. ~~**Sanitization**~~***Planning*****.** ~~Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing. IS resources shall be sanitized before they are released from classified information controls or released for use at a lower classification level.~~ *Contractors will develop, document, maintain, and implement security plans for ISs that describe the security controls in place or planned for the ISs and the rules of behavior for individuals accessing the ISs.*

c. ***Security Control Assessments****. As part of the assessment and self-inspection processes, the contractor will:*

(1) Assess the ISs security controls to determine if they are effective.

(2) Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities.

(3) Monitor ISs security controls on an ongoing basis to ensure continued effectiveness.

d. ***Program Management****.* The contractor will develop and implement an organization-wide information security program that supports the protection of classified information and ISs that process classified information that support the operations and assets of the contractor.

e. ***Risk Assessment****. The contractor will:*

(1) Categorize the potential impact level for confidentiality based on the classification level of the system (CONFIDENTIAL = Low; SECRET = Moderate; TOP SECRET = High).

(2) When required by contract, protect against the loss of availability or integrity, add the confidentiality impact level with the appropriate impact levels for integrity and availability to determine the security control baseline (e.g., Moderate, Low, Low). Otherwise, when the loss of availability and integrity is not required by contract, the security control baseline will be Low, Low.

(3) Document the security categorization results (including supporting rationale) in the systems security plan.

(4) Monitor changes to the ISs that may impact the security posture and the risk to the IS and its environment of operation (including the identification of new threats and vulnerabilities or other conditions that may impact the security state of the system). If changes occur, update the potential impact levels and inform the AO to determine if reauthorization is necessary.

- ~~Paragraph **8-302. Examination of Hardware and Software.** IS hardware and software shall be examined when received from the vendor and before being placed into use.~~ ***Operational Controls.*** *Operational controls are methods primarily implemented and executed by people (as opposed to systems) to improve system security. Contractors will apply the following Operational Control measures:*

a. ~~**IS Software** ***Personnel Security***~~**.** ~~Commercially procured software shall be tested to ensure that the software contains no obvious features that might be detrimental to the security of the IS. Security-related software shall be tested to verify that the security features function as specified.~~

(1) Individuals occupying positions of responsibility for classified ISs meet the security criteria established for those positions;

(2) Classified Information and ISs are protected during and after personnel actions, such as resignations, retirements, terminations, transfers, or loss of access to the system for cause, or the individual no longer has a reason to access the IS; in such circumstances, the individual's user ID and its authentication will be disabled or removed from the system and the account.

(3) The contractor is required to review audit logs in accordance with CSA-provided guidance, as a component of its continuous monitoring to determine if there are any personnel failing to comply with security policies and procedures and taking appropriate administrative actions. In addition, when circumstances warrant, the contractor will review audit logs, more immediately, if necessary, for inappropriate activity and employ appropriate administrative actions for personnel failing to comply with security policies and procedures.

b. ~~**IS Hardware**~~ ***Physical and Environmental Protection*****.** ~~Hardware shall be examined to determine that it appears to be in good working order and has no elements that might be detrimental to the secure operation of the IS when placed under facility control and cognizance. Subsequent changes and developments that affect security may require additional examination.~~

(1) Limit physical access into ISs operating environments to authorized individuals in accordance with reference (b).

(2) Protect the physical plant and support infrastructure for ISs.

(3) Provide supporting utilities for ISs, protect ISs against environmental hazards, and provide appropriate environmental controls in facilities containing ISs, when required by contract.

c. Contingency Planning*. When contractually required, contractors will establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery operations for ISs to ensure the availability of critical information and continuity of operations.*

d. Configuration Management*. Contractors will:*

(1) Establish and maintain baseline configurations and IS inventories (including hardware, software, firmware, and documentation) throughout the life cycles of these classified systems.

(2) Establish and enforce security configuration settings for information technology products employed in classified ISs, as prescribed by CSA guidelines.

e. Maintenance

(1) Perform necessary maintenance on classified ISs, including patch management.

(2) Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct classified ISs maintenance.

f. Classified ISs and Information Integrity

(1) Provide protection from malicious code at appropriate locations within classified ISs.

(2) Monitor IS security alerts and advisories that are accessible to contractors and take appropriate corrective action.

(3) Implement corrective measures to vulnerabilities identified by the GCA or CSA.

g. Media Protection

(1) Mark, label, and protect ISs media to the level of authorization until an appropriate classification review is conducted and resultant classification determination is made.

(2) Limit access to information on classified ISs media to authorized users.

(3) Sanitize or destroy ISs media before disposal or release for reuse in accordance with procedures established by the CSA.

h. Trusted Downloading. *When contractor program management determines that there is a valid requirement to perform trusted downloading procedures for moving media from a high to lower security domain (e.g., TOP SECRET to SECRET; SECRET to Unclassified), the contractor must follow established procedures approved by the CSA. If conditions exist that prevent the use of CSA*

established trusted download procedures, alternate technical and administrative procedures must be documented, reviewed, tested, and certified to work by the ISSM. The AO may require the ISSM to submit the alternate procedures to the GCA for endorsement before the AO makes a decision whether to approve the use of the alternate procedures. Performing the alternative approved procedures is considered an alternate trusted download.

i. Incident Response

(1) Implement CSA-provided auditing processes and procedures in order to detect security incidents involving ISs.

(2) Report immediately any such incidents to the CSA.

(3) Respond to and mitigate incidents in accordance with CSA guidance.

j. Awareness and Training. *The contractor will ensure personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. When the results of the CSA's oversight indicate deficiencies in training or technical competence on the part of the ISSM or ISSO, the contractor will take appropriate corrective action.*

- ~~Paragraph 8-303. **Identification and Authentication Management.** As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.~~ ***Technical Controls.*** *Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse; facilitate detection of security violations; and support security requirements for applications and data. Contractors will apply the following technical control measures:*

a. ~~**Unique**~~ **Identification** ***and Authentication*****.** ~~Each user shall be uniquely identified and that identity shall be associated with all auditable actions taken by that individual.~~ *Contractors will identify ISs users, processes acting on behalf of users, or devices and then will authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to ISs. The CSA will provide direction on the length and content of passwords.*

b. ~~**Authentication at Logon.** Users shall be required to authenticate their identities at "logon" time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior~~

~~to the execution of any application or utility on the system.~~ ***Access Control.*** *Contractors will limit ISs access to authorized users, processes acting on behalf of authorized users, or authorized devices (including other ISs). Access must be limited to the types of transactions and functions that authorized users are permitted to exercise.*

c. ~~**Applicability of Logon Authentication.** In some cases, it may not be necessary to use IS security controls as logon authenticators. In the case of stand alone workstations, or small local area networks, physical security controls and personnel security controls may suffice. For example, if the following conditions are met, it may not be necessary for the IS to have a logon and password:~~ ***Audit and Accountability***

(1) ~~The workstation does not have a permanent (internal) hard drive, and the removable hard drive and other associated storage media are stored in an approved security container when not in use.~~ *Create, protect, and retain ISs audit records to the extent needed to enable the monitoring, review and analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate ISs activity.*

(2) ~~All of the users with access to the workstation and the security container/ removable media have the required clearance level and need-to-know for all of the data processed on the workstation.~~ *Uniquely trace the actions of individual ISs users so they can be held accountable for their actions.*

~~(3) The workstation is located within an approved security area, and all uncleared/lower-cleared personnel are escorted within the area.~~

d. ~~**Access to Authentication Data.** Access to authentication data shall be restricted to authorized personnel through the use of encryption or file access controls, or both.~~ ***System and Communications Protection***

(1) Monitor, control, and protect organizational communications (i.e., information transmitted or received by the IS) at the external boundaries and key internal boundaries of the IS.

(2) Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security.

~~e. **User ID Reuse.** Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) shall be removed from the system.~~

f. **User ID Removal.** When an employee terminates, loses access to the system for cause, or no longer has a reason to access the IS, that individual's user ID and its authentication shall be disabled or removed from the system.

g. **User ID Revalidation.** Active user IDs are revalidated at least annually.

h. **Protection of Individual Authenticator.** An authenticator that is in the form of knowledge (password) or possession (smart card, keys) shall not be shared with anyone.

i. **Protection of Individual Passwords.** When passwords are used as authenticators, the following shall apply:

(1) Passwords shall be protected at a level commensurate with the sensitivity level or classification level and classification category of the information to which they allow access.

(2) Passwords shall contain a minimum of eight non-blank characters, shall be valid for no longer than 12 months and changed when compromised.

(3) Passwords shall be generated by a method approved by the CSA. Password acceptability shall be based on the method of generation, the length of the password, password structure, and the size of the password space. The password generation method, the length of the password, and the size of the password space shall be described in an attachment to the SSP.

(4) When an IS cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password.

(5) User software, including operating system and other security-relevant software, comes with a few standard authenticators (e.g., SYSTEM, TEST, and MASTER) and passwords already enrolled in the system. The ISSO shall ensure that the passwords for all standard authenticators are changed before allowing the general user population access to the IS. The ISSO shall also ensure that these passwords are changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.

- Paragraph 8-304. **Maintenance.** IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the

~~maintenance person's access to classified information and facilities.~~ ***Special Categories.*** *Several categories of ISs (e.g., tactical, embedded ISs, or special purpose systems) can be adequately secured with compensating security controls. Compensating security controls cover the management, operational, or technical controls of the ISs. Compensating security controls, which provide equivalent or comparable ISs protection, may be employed in lieu of prescribed security control baselines when approved by the CSA.*

a. The contractor will select the compensating controls from those described in the CSA-provided guideline set of security controls, and provide to the AO a complete rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the ISs.

b. The AO assesses the risk of operating the special categories ISs with the contractor's recommended set of compensating security controls. If the AO determines the risk is too high, the AO may require the contractor to request GCA acknowledgement that the GCA understands the risk associated with implementation of the contractor's proposed set of compensating security controls. Should the GCA also determine the risk is too high, it may recommend alternate or additional compensating security controls to the contractor and the AO, or recommend that the AO not authorize the system in its present security configuration.

c. The contractor may also obtain additional compensating controls from the GCA, if recommended by the GCA.

d. The contractor then resubmits to the AO for a final authorization decision, including the GCA's acknowledgement decision in accordance with paragraph 8-304b of this chapter with the contractor's initial set of compensating security controls. The contractor must also include the GCA's additional recommended compensating controls, if any were provided, in accordance with paragraph 8-304c of this chapter.

~~a~~*e*. ~~**Cleared Maintenance** ***Personnel.*** Maintenance personnel who are cleared to the highest classification level of information on the system and indoctrinated for all information processed on that system do not require an escort, if need-to-know controls can be implemented. When possible, an appropriately cleared and technically knowledgeable, facility employee shall be present within the area where the maintenance is being performed to ensure that security procedures are being followed.~~ ***Tactical, Embedded, Data-acquisition, Legacy, and Special-purpose Systems.*** *Tactical, embedded, data-acquisition, legacy, and special-purpose systems are special categories of systems requiring alternative set of controls not readily available in typical systems. Some ISs are incapable of*

alteration by users and are designed and implemented to provide a very limited set of predetermined functions. These systems are considered members of a special category, as are data-acquisition systems and other special-purpose test type systems. If an IS meets the criteria of a legacy IS (i.e., incapable of meeting the baseline security control requirements), authorization for continued use of a legacy IS may be granted when the benefits of upgrading the IS to meet baseline security controls do not outweigh the benefits of the additional controls and continued technological enhancements.

~~b~~*f*. ~~**Uncleared (or Lower-Cleared) Maintenance Personnel**~~ ***Mobile Systems*****.**

~~(1) If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided an appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Uncleared maintenance personnel must be U.S. citizens.~~

~~(2) System initiation and termination shall be performed by the escort. In addition, keystroke monitoring shall be performed during access to the system.~~

~~(3) Prior to maintenance, the IS shall be completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured. When a system cannot be cleared procedures, which are identified in the SSP, shall be enforced to deny the maintenance personnel visual and electronic access to any classified data contained on the system.~~

~~(4) A separate, unclassified copy of the operating system, including any micro-coded floppy disks, CD-ROM, or cassettes that are integral to the operating system, shall be used for all maintenance operations. The copy shall be labeled "UNCLASSIFIED -- FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSP. Maintenance procedures for an IS using a non-removable storage device on which the operating system is resident shall be considered by the ISSM on a case-by-case basis~~*Mobile systems may be periodically relocated to another cleared contractor facility or government site. A mobile system may be a complete system or components of a larger more complex system. Special procedures are required to document applicability, control and account for the movement, operations, and security of systems that are relocated to alternative locations. When a mobile system requires relocation, the contractor must provide the CSA with sufficient notice before the date of relocation. The contractor must submit to the CSA a mobile processing plan that addresses all aspects of security and includes*

secure movement, physical security, and operations at the new location before relocation.

- Paragraph **8-305. Malicious Code.** Policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, shall be implemented. All files must be checked for viruses before being introduced on an IS and checked for other malicious code as feasible. The use of personal or public domain software is strongly discouraged. Each installation of such software must be approved by the ISSM.

- Paragraph **8-306. Marking Hardware, Output, and Media.** Markings on hardware, output, and media shall conform to Chapter 4 of this manual. If the required marking is impractical or interferes with the operation of the media, the CSA may approve alternate marking procedures.

  a. **Hardware Components.** All components of an IS, including input/output devices that have the potential for retaining information, terminals, stand-alone microprocessors, or word processors used as terminals, shall bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the IS. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the IS and displayed on the screen. If the CSA requires that labels be color coded to indicate classification level they shall be orange for Top Secret, red for Secret, blue for Confidential, and green for unclassified.

  b. **Hard Copy Output and Removable Media.** Hard copy output (paper, fiche, film, and other printed media) and removable media shall be marked with visible, human readable, external markings to the accreditation level of the IS unless an appropriate classification review has been conducted or in the case of media, the information has been generated by a tested program verified to produce consistent results and approved by the CSA. Such programs will be tested on a statistical basis to ensure continuing performance.

  c. **Unclassified Media.** In the CSA-approved areas where classified and unclassified information are processed on collocated IS, unclassified media shall be so marked.

- Paragraph **8-307. Personnel Security.** Personnel with system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one

~~individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.~~

- ~~Paragraph **8-308. Physical Security**~~

  ~~a. Safeguards shall be established that prevent or detect unauthorized access to the IS and unauthorized modification of the IS hardware and software. Hardware integrity of the IS, including remote equipment, shall be maintained at all times, even when all classified information has been removed from the IS.~~

  ~~b. Classified processing shall take place in a CSA-approved area.~~

  ~~c. Visual Access. Devices that display or output information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information.~~

  ~~d. Unescorted Access. All personnel granted unescorted access to the area containing the IS shall have an appropriate security clearance.~~

- ~~Paragraph **8-309. Protection of Media.** Media must be protected to the level of accreditation until an appropriate classification review has been conducted.~~
- ~~Paragraph **8-310. Review of Output and Media**~~

  ~~a. **Human-Readable Output Review.** An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.~~

  ~~b. **Media Review.** Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. CSA-approved random or representative sampling techniques may be used to verify the proper marking of large volumes of output.~~

- ~~Paragraph **8-311. Configuration Management.** Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system~~

maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

a. **Configuration Documentation.** Procedures shall be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security-relevant software product names and version or release numbers, and physical location.

b. **System Connectivity.** Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.

c. **Connection Sensitivity.** The sensitivity level of each connection or port controlled by the Security Support Structure (SSS) shall be documented.

d. **CM Plan.** The facility CM program shall be documented in a CM plan and shall include:

(1) Formal change control procedures to ensure the review and approval of security-relevant hardware and software.

(2) Procedures for management of all documentation, such as the SSP and security test plans, used to ensure system security.

(3) Workable processes to implement, periodically test, and verify the CM plan.

(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

- **Section 4. Protection Measures**

  - Paragraph **8-400. Protection Profiles.** Protection profiles required for a particular IS are determined by the Level of Concern for Confidentiality and by the operating environment of the system as reflected by the clearances, access approvals and need-to-know embodied in the user environment. Operational data integrity and system availability, while important security concerns, are not covered by the NISP and will be determined in additional guidance or requirements issued by the GCA. However, provisions for integrity and availability concerns are included in this Chapter to provide guidance when the GCA contractually imposes them.

- Paragraph **8-401. Level of Concern**. The level of concern reflects the sensitivity of the information and the consequences of the loss of confidentiality, integrity or availability.

  a. **Information Sensitivity Matrices.** The matrices presented in Tables 1, 2, and 3 are designed to assist the CSA, with input from the ISSM in determining the appropriate protection level for confidentiality, and the level of concern for integrity, and availability, if contractually mandated, for a given IS processing a given set of information. The Information Sensitivity Matrices should be used as follows:

    (1) A determination of high, medium, or basic shall be made for each of the three attributes: confidentiality, integrity, and availability. It is not necessary for the level of concern to be the same for all attributes of the system.

    (2) When multiple applications on a system result in different levels of concern for the categories of confidentiality, integrity and availability the highest level of concern for each category shall be used.

  b. **Confidentiality Level of Concern.** In considering confidentiality, the principal question is the necessity for supporting the classification levels and the categories of information (e.g., Secret National Security Information) on the system in question. The Protection Level Table for Confidentiality (Table 4) combines the processing environment with the level of concern for confidentiality to provide a Protection Level. The Protection Level is then applied to Table 5 to provide a set of graded requirements to protect the confidentiality of the information on the system.

  c. **Integrity Level of Concern.** In considering integrity, the principal question is the necessity for maintaining the integrity of the information on the system in question.

  d. **Availability Level of Concern.** In considering availability, the principal consideration is the need for the information on the system in question to be available in a fixed time frame to accomplish a mission.

- Paragraph **8-402. Protection Level.** The protection level of an IS is determined by the relationship between two parameters: first, the clearance levels, formal access approvals, and need-to-know of users; and second, the level of concern based on the classification of the data on a particular system. The protection level translates into a set of requirements (tables 5, 6, and 7) that must be implemented

in the resulting system. Table 4 presents the criteria for determining the following three protection levels for confidentiality.

a. Systems are operating at Protection Level 1 when all users have all required approvals for access to all information on the system. This means that all users have all required clearances, formal access approvals, and the need-to-know for all information on the IS, i.e. dedicated mode.

b. Systems are operating at Protection Level 2 when all users have all required clearances, and all required formal access approvals, but at least one user lacks the need-to-know for some of the information on the system, i.e. a system high mode.

c. Systems are operating at Protection Level 3 when all users have all required clearances, but at least one user lacks formal access approval for some of the information on the system, i.e. compartmented mode.

- Paragraph **8-403.Protection Profiles.** Protection requirements graded by levels of concern and confidentiality protection level are detailed in Section 6. Tables 5, 6, and 7 present the requirements detailed in Section 6. To use these tables, find the column representing the protection level for confidentiality, or, if contractually mandated, find the column representing the level of concern for integrity or availability.

  a. **Confidentiality Components.** Confidentiality components describe the confidentiality protection requirements that must be implemented in an IS using the profile. The confidentiality protection requirements are graded according to the confidentiality protection levels.

  b. **Integrity Components.** Integrity components, if applicable, describe the integrity protection requirements that must be implemented in an IS using the profile. The integrity protection requirements are graded according to the integrity level of concern.

  c. **Availability Components.** Availability components, if applicable, describe the availability protection requirements that must be implemented in an IS using the profile. The availability protection requirements are graded according to the availability level of concern.

- **Table 1. Information Sensitivity Matrix for Confidentiality**

Level of Concern	Qualifiers

~~High~~	~~TOP SECRET and SECRET Restricted Data (SIGMAs 1,2,14,15)~~
~~Medium~~	~~SECRET~~ ~~SECRET Restricted Data~~
~~Basic~~	~~CONFIDENTIAL~~

- **~~Table 2. Information Sensitivity Matrix for Integrity~~**

~~Level of Concern~~	~~Qualifiers~~
~~High~~	~~Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.~~
~~Medium~~	~~High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.~~
~~Basic~~	~~Reasonable degree of accuracy required for mission accomplishment.~~

- **~~Table 3. Information Sensitivity Matrix for Availability~~**

~~Level of Concern~~	~~Qualifiers~~
~~High~~	~~Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.~~
~~Medium~~	~~Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability;~~

	or loss of availability will have an adverse effect on organizational-level interests.
Basic	Information must be available with flexible tolerance for delay.

- NOTE: In this context, "High - no tolerance for delay" means no delay; "Medium - minimum tolerance for delay" means a delay of seconds to hours; and "Basic - flexible tolerance for delay" means a delay of days to weeks. In the context of the NISPOM, integrity and availability shall only apply when the have a direct impact on protection measures for confidentiality, i.e., integrity of the password file, integrity of audit logs or when contractually imposed.

- **Table 4. Protection Level Table for Confidentiality**

Level of Concern	Lowest Clearance	Formal Access Approval	Need-To-Know	Protection Level
High, Medium, or Basic	At Least Equal to Highest Data	NOT ALL Users Have ALL	Not contributing to the decision	3
High, Medium, or Basic	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	2
High, Medium, or Basic	At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	1

- **Table 5. Protection Profile Table for Confidentiality**

	Confidentiality Protection Level		
Requirements (Paragraph)	P L 1	PL 2	PL 3
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3 Audit 4
Data Transmission (8-605)	Trans 1	Trans 1	Trans 1

~~Access Controls (8-606)~~	~~Access 1~~	~~Access 2~~	~~Access 3~~
~~Identification & Authentication (8-607)~~	~~I&A 1~~	~~I&A 2,3,4~~	~~I&A2,4,5~~
~~Resource Control (8-608)~~		~~ResrcCtrl 1~~	~~ResrcCtrl 1~~
~~Session Controls (8-609)~~	~~SessCtrl 1~~	~~SessCtrl 2~~	~~SessCtrl 2~~
~~Security Documentation (8-610)~~	~~Doc 1~~	~~Doc 1~~	~~Doc 1~~
~~Separation of Functions (8-611)~~			~~Separation~~
~~System Recovery (8-612)~~	~~SR 1~~	~~SR 1~~	~~SR 1~~
~~System Assurance (8-613)~~	~~SysAssur 1~~	~~SysAssur 1~~	~~SysAssur 2~~
~~Security Testing (8-614)~~	~~Test 1~~	~~Test 2~~	~~Test 3~~

- ~~**Table 6. Protection Profile Table for Integrity**~~

	~~Integrity Level of Concern~~		
~~Requirements (Paragraph)~~	~~Basic~~	~~Medium~~	~~High~~
~~Audit Capability (8-602)~~	~~Audit 1~~	~~Audit 2~~	~~Audit 3~~
~~Backup and Restoration of Data (8-603)~~	~~Backup 1~~	~~Backup 2~~	~~Backup 3~~
~~Changes to Data (8-604)~~		~~Integrity 1~~	~~Integrity 2~~
~~System Assurance (8-613)~~		~~SysAssur 1~~	~~SysAssur 2~~
~~Security Testing (8-614)~~	~~Test 1~~	~~Test 2~~	~~Test 3~~

- ~~**Table 7. Protection Profile Table for Availability**~~

	~~Availability Level of Concern~~

Requirements (Paragraph)	Basic	Medium	High
Alternate Power Source (8-601)		Power 1	Power 2
Backup and Restoration of Data (8-603)	Backup 1	Backup 2	Backup 3

- **Section 5. Special Categories.**

  - Paragraph **8-500. Special Categories.** Several categories of systems can be adequately secured without implementation of all the technical features specified this Chapter. These systems are not "exceptions" or "special cases" but applying the technical security requirements to these systems by rote results in unnecessary costs and operational impacts. In general, the technical questions are where, when, and how to apply a given set of protection measures, rather than whether to apply the measures. For many of these "special" systems (such as guards or pure servers; and tactical, embedded, data-acquisition, and special-purpose systems), the physical security protections for the system provide the required access control, while the application running on the platform provides the required user separation.

  - Paragraph **8-501. Single-user, Stand-alone Systems**. Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. The CSA can approve administrative and environmental protection measures for such systems, in lieu of technical ones. Systems that have one user at a time, but have a total of more than one user with no sanitization between users, are multi-user systems, and the CSA shall consider the systems as such in determining the protection level and the resulting security requirements. Systems that have one user at a time, are sanitized between users and periods of different classification/sensitivity, are periods processing systems as described below.

  - Paragraph **8-502. Periods Processing.** Periods processing is a method of sequential operation of an IS that provides the capability to process information at various levels of sensitivity at distinctly different times.

    a. Periods processing provides the capability to either have more than one user or group of users (sequentially) on a single-user IS who do not have the same need-to-know or who are authorized to access different levels of information; or use an IS at more than one protection level (sequentially).

    b. Sanitization After Use. If an IS is used for periods processing either by more than one user or for segregating information by classification level onto separate

~~media, the SSP shall specify the sanitization procedures to be employed by each user before and after each use of the system.~~

~~c. Sanitization Between Periods. The IS shall be sanitized of all information before transitioning from one period to the next (e.g., whenever there will be a new user(s) who does not have an access authorization or need-to-know for data processed during the previous period, changing from one protection level to another). These procedures shall be documented in the SSP. Such procedures could include, among others, sanitizing non-volatile storage, exchanging disks, and powering down the IS and its peripherals.~~

~~d. Media For Each Period. An IS employed in periods processing shall have separate media for each period of processing, including copies of operating systems, utilities, and applications software.~~

~~e. Audit. If there are multiple users of the system and the system is not capable of automated logging, the CSA shall consider requiring manual logging. Audit trails are not required for single-user stand-alone systems.~~

- ~~Paragraph **8-503. Pure Servers**~~

~~a. Certain specialized systems, when acting as pure servers in a network, do not fit the protection level criteria and may need fewer technical security countermeasures. These systems have the following characteristics:~~

~~(1) No user code is present on the system.~~

~~(2) Only system administrators and maintainers can access the system.~~

~~(3) The system provides non-interactive services to clients (e.g., packet routing or messaging services).~~

~~(4) The hardware and/or application providing network services otherwise meet the security requirements of the network.~~

~~(5) The risk of attack against the Security Support Structure (SSS) using network communication paths is sufficiently low.~~

~~(6) The risk of attack against the SSS using physical access to the system itself is sufficiently low.~~

~~b. The platform (i.e., hardware and operating system) on which the guard or pure server runs usually needs to meet no more than Protection Level 3 security requirements. The guard or pure server may have a large number of clients (i.e.,~~

~~individuals who use the guard or server functional capabilities in a severely constrained way). The guard application or server application itself will have to provide the more stringent technical protections appropriate for the system's protection level and operational environment. Assurances appropriate to the levels of concern for the system shall be implemented.~~

~~c. Systems that have general users or execute general user code are not "pure servers" within the meaning of this section, and so must meet all security requirements specified for their protection level and operational environment.~~

~~d. The term "pure server" is not intended to limit the applicability of this section to systems that have traditionally been referred to as servers. For example, a messaging system that happened to be implemented on a general-purpose computer platform could be accredited under this section and, if such a system meets the specifications in a, above, the system's technical requirements could be categorized by this section.~~

~~e. The above easing of technical security requirements does not imply any relaxation in other security requirements (e.g., physical and communications security requirements) which are determined by the information handled or protected by the system. As stated above, this easing of technical requirements is predicated upon adequate application of physical security and other appropriate security disciplines.~~

- ~~Paragraph **8-504. Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems.** Some systems are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called "embedded" systems fall into this category, as do some data-acquisition systems and some other special-purpose systems. These systems also have the characteristics that: first and most importantly, there are no general users on the system; and, second, there is no user code running on the system. If the CSA determines that such a system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this section. The CSA and implementers are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system's protection level.~~

- ~~Paragraph **8-505. Systems with Group Authenticators**. Many security measures specified in this section implicitly assume that the system includes an acceptable level of individual accountability. This is normally ensured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/ authenticator combination. Such situations are often referred to as requiring the use of group~~

authenticators. In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators shall be used only for broader access after the use of a unique authenticator for initial identification and authentication, and documented in SSP. Group authenticators may not be shared with anyone outside of the group.

- **Section 6. Protection Requirements**

  - Paragraph **8-600. Introduction.** This section describes the implementation requirements for different protection measure.

  - Paragraph **8-601. Alternate Power Source (Power).** An alternate power source ensures that the system availability is maintained in the event of a loss of primary power. An APS can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.

    a. **Power 1 Requirements.** Procedures for the graceful shutdown of the system shall ensure no loss of data. The decision not to use an alternate source of power, such as an uninterruptible power supply (UPS) for the system, shall be documented.

    b. **Power 2 Requirements.** Instead of Power 1, procedures for transfer of the system to another power source shall ensure that the transfer is completed within the time requirements of the application(s) on the system.

  - Paragraph **8-602. Audit Capability.** Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

    a. **Audit 1 Requirements**

      (1) Automated Audit Trail Creation: The system shall automatically create and maintain an audit trail or log (On a PL-1 system only: In the event that the Operating System cannot provide an automated audit capability, an alternative method of accountability for user activities on the system shall be developed and documented.) Audit records shall be created to record the following:

        (a) Enough information to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity

~~that initiated or completed the action, the resources involved, and the action involved.~~

~~(b) Successful and unsuccessful logons and logoffs.~~

~~(c) Successful and unsuccessful accesses to security relevant objects and directories, including creation, open, close, modification, and deletion.~~

~~(d) Changes in user authenticators.~~

~~(e) The blocking or blacklisting of a user ID, terminal, or access port and the reason for the action.~~

~~(f) Denial of access resulting from an excessive number of unsuccessful logon attempts.~~

~~(2) Audit Trail Protection. The contents of audit trails shall be protected against unauthorized access, modification, or deletion.~~

~~(3) Audit Trail Analysis. Audit analysis and reporting shall be scheduled, and performed. Security relevant events shall be documented and reported. The frequency of the review shall be at least weekly and shall be documented in the SSP.~~

~~(4) Audit Record Retention. Audit records shall be retained for at least one review cycle or as required by the CSA.~~

~~b. **Audit 2 Requirements.** In addition to Audit 1:~~

~~(1) Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual). Periodic testing by the ISSO or ISSM of the security posture of the IS~~

~~c. **Audit 3 Requirements.** In addition to Audit 2:~~

~~(1) Automated Audit Analysis. Audit analysis and reporting using automated tools shall be scheduled and performed.~~

~~d. **Audit 4 Requirements.** In addition to Audit 3:~~

~~(1) An audit trail, created and maintained by the IS, that is capable of recording changes to mechanism's list of user formal access permissions.~~

- Paragraph **8-603. Backup and Restoration of Data (Backup).** The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

  a. **Backup 1 Requirements**

  (1) Backup Procedures. Procedures for the regular backup of all essential and security-relevant information, including software tables and settings, such as router tables, software, and documentation, shall be documented.

  (2) Backup Frequency. The frequency of backups shall be defined by the ISSM, with the assistance of the GCA, and documented in the backup procedures.

  b. **Backup 2** Requirements. In addition to Backup 1:

  (1). Backup Media Storage. Media containing backup files and backup documentation shall be stored at another location, such as another part of the same building, a nearby building, or off facility, so as to reduce the possibility that a common occurrence could eliminate the on-facility backup data and the off-facility backup data.

  (2) Verification of Backup Procedures. Backup procedures shall be periodically verified.

  c. **Backup 3 Requirements.** In addition to Backup 2:

  (1) Information Restoration Testing. Incremental and complete restoration of information from backup media shall be tested on an annual basis.

- Paragraph **8-604. Changes to Data (Integrity).** The control of changes to data includes deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized changes are allowed.

  a. **Integrity 1 Requirements**

  (1) Change Procedures. Procedures and technical system features shall be implemented to ensure that changes to the data and IS software are executed only by authorized personnel or processes.

  b. **Integrity 2 Requirements.** In addition to Integrity 1:

(1) Transaction Log. A transaction log, protected from unauthorized changes, shall be available to allow the immediate correction of unauthorized data and IS software changes and the off-line verification of all changes at all times.

- Paragraph **8-605. Data Transmission (Trans).** Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).

a. **Trans 1 Requirements**

(1) Protections. One or more of the following protections shall be used.

(a) Information distributed only within an area approved for open storage of the information.

(b) NSA-approved encryption mechanisms appropriate for the encryption of classified information.

(c) Protected Distribution System.

- Paragraph **8-606. Access Controls (Access).** The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.

a. **Access 1 Requirements**

(1) Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

b. **Access 2 Requirements.** In addition to Access 1:

(1) Discretionary access controls shall be provided. A system has implemented discretionary access controls when the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The discretionary access control policy includes administrative procedures to support the policy and its mechanisms.

c. **Access 3 Requirements.** In addition to Access 2:

(1) Some process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals granted to another user.

(2) Some process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data.

- Paragraph **8-607. Identification and Authentication (I&A)**

a. **I&A 1Requirements.** Procedures that include provisions for uniquely identifying and authenticating the users. Procedures can be external to the IS (e.g., procedural or physical controls) or internal to the IS (i.e., technical). Electronic means shall be employed where technically feasible.

b. **I&A 2 Requirements.** In addition to I&A 1:

(1) An I&A management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified in the SSP:

(a) Initial authenticator content and administrative procedures for initial authenticator distribution.
(b) Individual and Group Authenticators. Group authenticators may only be used in conjunction with an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator.

(c) Length, composition and generation of authenticators.

(d) Change processes (periodic and in case of compromise.

(e) Aging of static authenticators (i.e., not one-time passwords or biometric patterns).

(f) History of authenticator changes, with assurance of non-replication of individual authenticators.

(g) Protection of authenticators.

c. **I&A 3 Requirements.** In addition to I&A 2:

(1) Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links that are outside the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks.)

d. **I&A 4 Requirements.** In those instances where the means of authentication is user-specified passwords, the ISSM may employ (with the approval of the CSA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover the user's password.

e. **I&A 5 Requirements.** In those instances where the users are remotely accessing the IS, the users shall employ a strong authentication mechanism.

- Paragraph **8-608. Resource Control (ResrcCtrl)** The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.

- Paragraph **8-609. Session Controls (SessCtrl).** Session controls are requirements, over and above identification and authentication, for controlling the establishment of a user's session.

a. **SessCtrl 1 Requirements**

(1) User Notification. All users shall be notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit. The user shall also be advised that, by using the system, he/she has granted consent to such monitoring and recording. The user shall also be advised that unauthorized use is prohibited and subject to criminal and civil penalties. If the operating system permits, each initial screen (displayed before user logon) shall contain a warning text to the user and the user shall be required to take positive action to remove the notice from the screen (monitoring and recording, such as collection and analysis of audit trail information, shall be performed). The CSA will provide an approved banner. If it is not possible to provide an "initial screen" warning notice, other methods of notification shall be developed and approved by the CSA.

(2) Successive Logon Attempts. If the operating system provides the capability, successive logon attempts shall be controlled as follows:

(a) By denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same user ID.

(b) By limiting the number of access attempts in a specified time period.

(c) By the use of a time delay control system.

(d) By other such methods, subject to approval by the CSA.

(3) System Entry. The system shall grant system entry only in accordance with the conditions associated with the authenticated user's profile. If no explicit entry conditions are defined, the default shall prohibit all remote activities, such as remote logons and anonymous file access.

b. **SessCtrl 2 Requirements.** In addition to SessCtrl 1:

(1). Multiple Logon Control. If the IS supports multiple logon sessions for each user ID or account, the IS shall provide a protected capability to control the number of logon sessions for each user ID, account, or specific port of entry. The IS default shall be a single logon session.

(2). User Inactivity. The IS shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the SSP.

(3). Logon Notification. If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

- Paragraph **8-610. Security Documentation (Doc).** Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.

a. **Doc 1 Requirements**

(1) SSP. The SSP shall contain the following:

(a) System Identification.

1. Security Personnel. The name, location, and phone number of the responsible system owner, CSA, ISSM, and ISSO.

2. Description. A brief narrative description of the system or network mission or purpose and architecture, including subnetworks, communications devices, and protocols.

(b) System Requirements Specification.

1. Sensitivity and Classification Levels. The sensitivity or classification levels, and categories of all information on the system and clearance, formal access approval and need-to-know of IS users.

2. Levels of Concern for Confidentiality, Integrity, and Availability. The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern.

3. Protection Measures. Identify protection measures and how they are being met.

4. Variances from Protection Measure Requirements. A description of any approved variances from protection measures. A copy of the approval documentation shall be attached to the SSP.

(c) System-Specific Risks and Vulnerabilities. A description of the risk assessment of any threats or vulnerabilities unique to the system. If there are no threats or vulnerabilities unique to the facility or system, a statement to that effect shall be entered. If any vulnerabilities are identified by the assessment of unique threats, the countermeasures implemented to mitigate the vulnerabilities shall be described.

(d) System Configuration. A brief description of the system architecture, including a block diagram of the components that show the interconnections between the components and any connections to other systems, and an information flow diagram.

(e) Connections to Separately Accredited Networks and Systems. If connections to other systems exist, a memorandum of understanding is necessary if the systems are approved by a person other than the CSA responsible for this system. A copy of any memoranda of understanding with other agencies shall be attached to the SSP.

(f) Security Support Structure. A brief description of the security support structure including all controlled interfaces, their interconnection criteria, and security requirements.

~~(2) Certification and Accreditation Documentation.~~

~~(a) Security Testing. Test plans, procedures, and test reports including risk assessment.~~

~~(b) Documentation. The test plan for ongoing testing and the frequency of such testing shall be documented in the SSP.~~

~~(c) Certification. A certification statement that the system complies with the requirements of the protection level and levels of concern for this system. The statement shall be signed by the ISSM.~~

~~(d) Accreditation. Documentation for accreditation includes the certification package. The CSA approves the package and provides accreditation documentation.~~

- ~~Paragraph **8-611. Separation of Function Requirements (Separation).** At Protection Level 3 the functions of the ISSO and the system manager shall not be performed by the same person.~~

- ~~Paragraph **8-612. System Recovery (SR).** System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition where all security-relevant functions are operational or system operation is suspended.~~

  ~~a. **SR 1 Requirements.** Procedures and IS features shall be implemented to ensure that IS recovery is done in a controlled manner. If any off-normal conditions arise during recovery, the IS shall be accessible only via terminals monitored by the ISSO or his /her designee, or via the IS console.~~

- ~~Paragraph **8-613. System Assurance (SysAssur).** System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system, (e.g. Security Support Structure).~~

  ~~a. **SysAssur 1 Requirements**~~

  ~~(1) Access to Protection Functions. Access to hardware/software/firmware that perform systems or security functions shall be limited to authorized personnel.~~

  ~~b. **SysAssur 2 Requirements.** In addition to SysAssur1:~~

  ~~(1) Protection Documentation. The protections and provisions of the SysAssur shall be documented.~~

(2) Periodic Validation of SysAssur. Features and procedures shall exist to periodically validate the correct operation of the hardware, firmware, and software elements of the SSS and shall be documented in the SSP.

c. **SysAssur 3 Requirements.** In addition to SysAssur2:

(1) SSS Isolation. The SSS shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modifying its code and data structures).

- Paragraph **8-614. Security Testing (Test).** Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.

a. **Test 1 Requirements.** Assurance shall be provided to the CSA that the system operates in accordance with the approved SSP and that the security features, including access controls and configuration management, are implemented and operational.

b. **Test 2 Requirements.** In addition to Test1:

(1) Written assurance shall be provided to the CSA that the IS operates in accordance with the approved SSP, and that the security features, including access controls, configuration management and discretionary access controls, are implemented and operational.

c. **Test 3 Requirements.** In addition to Test2:

(1) Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.

(a) A test plan and procedures shall be developed and shall include:

1. A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels of Concern for integrity and availability.

2. A detailed description of the assurances that have been implemented, and how this implementation will be verified.

3. An outline of the inspection and test procedures used to verify this compliance.

- Paragraph **8-615. Disaster Recovery Planning.** If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's

~~mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.~~

- ~~**Section 7. Interconnected Systems.**~~

  - Paragraph ~~**8-700. Interconnected Systems Management.** The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.~~

    ~~a. When connecting two or more networks, the CSA shall review the security attributes of each network (even if the networks are accredited at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.~~
    ~~b. A unified network is a connected collection of systems or networks that are accredited: (1) under a single SSP, (2) as a single entity, and (3) by a single CSA. Such a network can be as simple as a small stand-alone LAN operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single ISSO. Conversely, it can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy, accredited as a single entity by a single CSA. The perimeter of each network encompasses all its hardware, software, and attached devices. Its boundary extends to all of its users.~~

    ~~c. An interconnected network is comprised of two or more separately accredited systems and/or networks. Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating system or network has its own ISSO. The interconnected network shall have a controlled interface capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires accreditation as a unit.~~

    ~~d. Systems that process information at differing classification levels or with differing compartmentation (i.e., at least two kinds of information that require different formal access approvals) can be interconnected if:~~

      ~~(1) They are interconnected through a Controlled Interface (as defined below) that provides the separation appropriate to the combination of the level(s) and compartment(s) being processed on both systems; or~~

      ~~(2) Both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or~~

~~(3) Both systems are accredited to process the level(s) and compartment(s) of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.~~

~~e. Any IS connected to another system that does not meet either d (2) or d (3) above shall utilize a Controlled Interface(s) (CI) that performs the following:~~

~~(1) A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.~~

~~(2) A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.~~
~~(3) Communications from outside the system perimeter shall have an authorized user as the addressee (i.e., the CI shall notify the user of the communication and forward the communication only on request from the user). If classified information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.~~

- ~~Paragraph~~ ~~**8-701. Controlled Interface Functions**~~

~~a. The functions of the CI include:~~

~~(1) Providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts.~~

~~(2) Providing a reliable exchange of security-related information.~~

~~(3) Filtering information in a data stream based on associated security labels for data content.~~

~~b. CIs have several characteristics including the following:~~

~~(1) There are no general users on the CI.~~

~~(2) There is no user code running on the CI.~~

~~(3) The CI provides a protected conduit for the transfer of user data.~~

~~(4) Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.~~

- ~~Paragraph **8-702. Controlled Interface Requirements.** The CI shall have the following properties:~~

  ~~a. Adjudicated Differences. The CI shall be implemented to monitor and enforce the protection requirements of the network and to adjudicate the differences in security policies.~~

  ~~b. Routing Decisions. The CI shall base its routing decisions on information that is supplied or alterable only by the SSS.~~

  ~~c. Restrictive Protection Requirements. The CI shall support the protection requirements of the most restrictive of the attached networks or IS.~~

  ~~d. User Code. The CI shall not run any user code.~~

  ~~e. Fail-secure. The CI shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.~~

  ~~f. Communication Limits. The CI shall ensure that communication policies and connections that are not explicitly permitted are prohibited.~~

  ~~g. In general, such systems have only privileged users; i.e., system administrators and maintainers. The CI may have a large number of clients (i.e., individuals who use the CI's functional capabilities in a severely constrained way). The CI application itself will have to provide the more stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the CI if each application (and the resources associated with it) is protected from unauthorized access or circumvention from other applications or users.~~

- ~~Paragraph 8-703. **8-703. Assurances for CIs.** Each CI shall be tested and evaluated to ensure that the CI, as implemented, can provide the separation required for the system's protection level. Specifically, the platform on which the CI runs does not necessarily have to provide the needed separation alone.~~

CHAPTER 9, SPECIAL REQUIREMENTS

- Chapter 9, Section 1 (Page 9-1-1): **RD, ~~*and*~~ FRD, *and Transclassified Foreign Nuclear Information (TFNI)***

  - ~~Paragraph 9-100: General. This section was prepared by DOE according to reference (a) and is provided for information purposes only. It describes the requirements for classifying and safeguarding nuclear-related information that is~~

~~designated RD or FRD or TFNI. Such information is classified under reference (c) as opposed to other Government information that is classified by E.O. (National Security Information (NSI)).~~ *See Appendix D, "NISPOM Supplement" of this Manual.*

- ~~Paragraph 9-101a: Reference (c) establishes policy for classifying and protecting RD, FRD, and TFNI information. Under section 141 of reference (c), DOE is responsible for controlling the dissemination and declassification of RD. Under section 142c and d of reference (c), DOE shares certain responsibilities regarding RD and FRD with the Department of Defense. Under section 142e of reference (c), DOE shares certain responsibilities regarding RD and TFNI with the DNI. Under section 143 of reference (c), the Secretary of Defense is responsible for establishing personnel and other security procedures and standards that are in reasonable conformity to the standards established by DOE. The procedures and standards established by the Secretary of Defense are detailed in other sections of the Manual and are applicable to contractors under the security cognizance of the Department of Defense.~~

- ~~Paragraph 9-101b: Specific policies and procedures for classifying and declassifying RD and FRD are set forth in 10 Code of Federal Regulations (CFR) Part 1045, Subparts A, B, and C (reference (p)).~~

- ~~Paragraph 9-101c: The Secretary of Energy and the Chairman of the NRC retain authority over access to information that is under their respective cognizance as directed by reference (c). The Secretary of DOE or the Chairman of the NRC may inspect and monitor contractor programs or facilities that involve access to such information or may enter into written agreement with the Department of Defense to inspect and monitor these programs or facilities.~~

- ~~Paragraph 9-102: **Unauthorized Disclosures.** Contractors shall report all unauthorized disclosures involving RD and FRD information to the CSA.~~

- ~~Paragraph 9-103: **International Requirements.** Reference (c) provides for a program of international cooperation to promote common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit. Under section 123 of reference (c), information controlled by reference (c) may be shared with another nation only under the terms of an agreement for cooperation. The disclosure by a contractor of RD and FRD shall not be permitted until an agreement is signed by the United States and participating governments and disclosure guidance and security arrangements are established. RD and FRD shall not be transmitted to a foreign national or regional defense organization unless such action is approved and undertaken under an agreement for cooperation between the United States and the~~

~~cooperating entity and supporting statutory determinations as prescribed in reference (c).~~

- ~~Paragraph 9-104: **Personnel Security Clearances**. Only DOE, NRC, Department of Defense, and NASA can grant access to RD and FRD. The minimum investigative requirements and standards for access to RD and FRD for contractors under the security cognizance of DOE are set forth below.~~

  ~~a. TOP SECRET RD – A favorable SSBI.~~

  ~~b. SECRET RD – A favorable SSBI.~~

  ~~c. CONFIDENTIAL RD – A favorable NACLC.~~

  ~~d. TOP SECRET FRD – A favorable SSBI.~~

  ~~e. SECRET FRD – A favorable NACLC.~~

  ~~f. CONFIDENTIAL FRD – A favorable NACLC.~~

- ~~Paragraph 9-105: **Classification.**~~

  ~~a. The Director, DOE, Office of Classification and Information Control, determines whether nuclear-related information is classified as RD under reference (p). DOE and the Department of Defense jointly determine what classified information is removed from the RD category to become FRD under section 14(a) of reference (p). These decisions are promulgated in classification guides issued under section 37(a) of reference (p).~~

  ~~b. Reference (p) describes the authorities and procedures for classifying RD and FRD information and documents. All contractors with access to RD and FRD shall designate specified employees as RD Classifiers. Only those contractor employees designated as RD classifiers may classify RD and FRD documents according to section 32(a)(2) of reference (p). Such employees must be trained on the procedures for classifying, declassifying, marking, and handling for RD and FRD information and documents according to section 35(a) of reference (p). RD classifiers shall use classification guides as the primary basis for classifying and declassifying documents containing RD and FRD information according to section 37(c) of reference (p). If such classification guidance is not available and the information in the document appears to meet the definition of RD, then the RD classifier shall, as an interim measure, mark the document as Confidential RD (or as Secret RD if the sensitivity of the information in the document so warrants) and promptly forward the document to the GCA. The GCA shall provide the contractor with the final determination based upon official published~~

~~classification guidance. If the GCA cannot make such a determination, the GCA shall forward the document to DOE for a classification determination according to section 14(a) of reference (p).~~

~~c. Classifying information as RD and FRD is not limited to U.S. Government information. Contractors who develop an invention or discovery useful in the production or utilization of special nuclear material or nuclear energy shall file a fully descriptive report with DOE or the Commissioner of Patents as prescribed by Section 151c of reference (c). Documents thought to contain RD or FRD shall be marked temporarily as such. These documents shall be promptly referred to the GCA for a final determination based upon official published classification guidance. If the GCA cannot make such a determination, the GCA shall forward the document to DOE for a classification determination.~~

- ~~Paragraphs 9-106, 9-107, 9-108 and 9-109~~
  - ~~9-106. Declassification.~~

    ~~a. DOE determines whether RD and TFNI information may be declassified under section 14(b) of reference (p). DOE, jointly with the Department of Defense, determines whether FRD information may be declassified under section 14(d) of reference (p).~~

    ~~b. Documents marked as containing RD, FRD and TFNI information remain classified until a positive action by an authorized Government official is taken to declassify them; no date or event for automatic declassification ever applies to RD, FRD, and TFNI documents.~~

  - ~~**9-107. Challenges to RD/FRD Classification**. Any contractor employee who believes that an RD, FRD, and TFNI document is classified improperly or unnecessarily may challenge that classification following the procedures established by the GCA.~~

  - ~~**9-108. Marking.** Documents containing RD, FRD, and TFNI information shall be marked as indicated below:~~

    ~~**a. Front of the Document.** In addition to the overall classification level of the document at the top and bottom of the page, the following notices must appear on the front of the document, as appropriate:~~

    ~~If the document contains RD information:~~

    ~~RESTRICTED DATA~~

~~This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.~~

~~If the document contains FRD information:~~

~~FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b, AEA 1954.~~

~~A document containing RD or FRD information also must be marked to identify: (1) the classification guide or source document (by title and date) used to classify the document and (2) the identity of the RD classifier unless the classifier is the same as the document originator or signer:~~

~~Derived from: (Classification guide or source document – title and date) RD Classifier: (Name and position or title).~~

~~**b. Interior Page**. Each RD or FRD document must also be clearly marked at the top and bottom of each interior page with the overall classification level and category of the document or the classification level and category of the page, whichever is preferred. The abbreviations RD and FRD may be used in conjunction with the classification level (e.g., SECRET RD or SECRET FRD).~~

~~**c. Other Caveats**. Any other caveats indicated on the source document shall be carried forward.~~

~~**d. TFNI.** Documents containing TFNI must be marked in accordance with rreference (z) and ISOO Notice 2011-02: Further Guidance and Clarification on Commingling Atomic Energy Information and Classification National Security Information
(reference (aa)).~~

- ~~Paragraph 9-109: **Comingling.** To the greatest degree possible, do not comingle RD and FRD in the same document with information classified pursuant to reference (b). When mixing can't be avoided, the requirements of references (b) and (z) must be met.~~

- ~~Chapter 9, Section 3 (Page 9-3-1):~~

  - ~~Paragraph **9-300. Background***General***.** This section was prepared by CIA in accordance with reference (a) and is provided for information purposes only. It contains general information on safeguarding intelligence information. Intelligence information is under the jurisdiction and control of the DNI, who~~

~~establishes security policy for the protection of intelligence information, sources, methods, and analytical processes.~~ ***General.*** *National intelligence is under the jurisdiction and control of the DNI, who establishes security policy for the protection of national intelligence and intelligence sources, methods, and activities. In addition to the guidance in this Manual, contractors shall follow IC directives, policy guidance, standards, and specifications for the protection of classified national intelligence and SCI. Contractors are not authorized to further disclose or release classified national intelligence and SCI (including to a subcontractor) without prior written authorization of the originating IC element.*

- ~~Paragraph **9-301. Definitions.** The following definitions pertain to intelligence information:~~

  ~~**a. Counterintelligence (CI)**. Information collection, analysis and operations conducted to identify and neutralize espionage, other foreign intelligence or covert actions, the intelligence related capabilities and activities of terrorists, and operations against U.S. personnel or political, economic and policy processes.~~

  ~~**b. Classified Intelligence Information.** Information identified as SCI included in SAPs for intelligence, and collateral classified intelligence information under the purview of the DNI.~~

  ~~**c. Foreign Intelligence.** Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence information except for information on international terrorist activities.~~

  ~~**d. Intelligence Community (IC).** Those U.S. Government organizations and activities identified as members of the IC in reference (e).~~

  ~~**e. Senior Officials of the Intelligence Community (SOICs).** SOICs are the heads of departments and agencies with organizations in the IC or the heads of IC organizations responsible for protecting classified intelligence information and intelligence sources and methods from unauthorized disclosure consistent with DNI policy.~~

  ~~**f. Senior Intelligence Officer (SIO).** The SIO is the highest ranking military or civilian individual charges with direct foreign intelligence missions, functions, or responsibilities within an element of the IC.~~

  ~~**g. SCI.** SCI is classified intelligence information concerning or derived from sensitive sources, methods, or analytical processes, which is required to be handled exclusively within formal access control systems established by the DNI.~~

h. SCI Facility (SCIF). A SCIF is an area, room, group of rooms, or installation accredited by the proper authority to store, use, discuss and/or process SCI.

- Paragraph **9-302. Key Concepts.** This section provides general guidance on the intended purpose of several security tenets that form a critical baseline for the protection of intelligence information.

a. Apply Need-to-Know. Authorized holders (individuals or information systems) of classified intelligence information shall determine if prospective recipients (individuals or information systems) have the requisite clearances and accesses, and require knowledge of specific classified intelligence information in order to perform or assist in a lawful and authorized governmental function. To effectively implement this concept, IC departments, agencies, and bureaus must work cooperatively with customers to understand their requirements and ensure that they receive all applicable classified intelligence information while minimizing the risk of unauthorized disclosure. IC organizations shall provide intelligence at multiple security levels appropriate to the security authorizations of intended customers. Customers, in turn, shall be responsible for verifying need-to-know for this information for individuals of information systems within their organizations.

b. Protect SCI. In order to protect information regarding particularly fragile intelligence sources and methods, SCI has been established as the SAP for the DNI. SCI must be protected in specific SCI control systems and shall be clearly defined and identified. The DNI has the sole authority to create or to discontinue SAPs, including SCI access control systems pertaining to intelligence sources and methods and classified intelligence activities (including special activities, but not including military operational, strategic, and tactical programs).

c. Educate the Work Force. SOICs shall establish formal security awareness training and education programs to ensure complete, common, and consistent understanding and application of security principles. Individuals shall be advised of their security responsibilities before receiving access to classified intelligence information and information systems. Annual refresher training is required to review security principles and responsibilities and to emphasize new security policies and practices developed from the preceding year.

d. Promote Security Reciprocity. To facilitate security reciprocity across the IC and industry, SOICs shall accept from other IC departments, agencies, and bureaus access eligibility determinations and accreditations of information systems and facilities except when an agency has documented information indicating that an employee, contractor, information system, or a facility does not meet DCID standards. Any exceptions to access eligibility determinations and

~~accreditations of information systems and facilities must be noted in certifications to other agencies.~~

~~**e. Promote Institutional Collaboration.** Security elements of the IC shall work with intelligence production, counterintelligence, and law enforcement partners to identify and implement integrated responses to threats. Proactive collaboration among programs should synergize efforts to protect the U.S. population, national security assets, and classified intelligence information.~~

~~**f. Manage Risk.** IC departments, agencies and bureaus shall employ a risk management/risk analysis process to cost-effectively minimize the potential for loss of classified intelligence information or assets and the consequences should such loss occur. This methodology shall involve techniques to counter threats, reduce vulnerabilities, and implement security countermeasures.~~

~~**g. Minimize Insider Threat.** All personnel who have access to classified intelligence information shall be thoroughly vetted, fully trained in their security responsibilities, appropriately supervised, and provided a secure work environment. CI and security management shall maintain aggressive programs to deter, detect, and support the apprehension and prosecution of those cleared personnel who endanger national security interests.~~

- ~~Paragraph **9-303 Control Markings Authorized for Intelligence Information**~~

~~**a. "DISSEMINATION AND EXTRACTION OF INFORMATION CONROLLED BY ORIGINATOR" (ORCON).** Information bearing this marking may be disseminated within the headquarters and specified subordinate elements of the recipient organizations, including their contractors within government facilities. This information may also be incorporated in whole or in part into other briefings or products, provided the briefing or product is presented or distributed only to original recipients of the information and marked accordingly. Dissemination beyond headquarters and specified subordinate elements or to agencies other than the original recipients requires advanced permission from the originator.~~

~~**b. "FOR OFFICIAL USE ONLY" (FOUO).** Intelligence information used to control dissemination of UNCLASSIFIED official government information until approved for public release by the originator. May be used only with UNCLASSIFIED on page markings.~~

~~**c. "CAUTION-PROPRIETARY INFORMATION INVOLVED" (PROPIN).** Marking used to identify information provided by a commercial firm or private source under an express or implied understanding that the information~~

~~will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This information may not be disseminated outside the Federal Government in any form without the express permission of the originator of the proprietary information. Dissemination to contractors is precluded irrespective of their status to, or within, the U.S. Government without the authorization of the originator of the information.~~

~~**d. "NOT Rreleasable TO FOREIGN NATIONALS" (NOFORN).** NOFORN is classified information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator. It cannot be used with REL TO [country codes] or EYES ONLY on page markings. When a document contains both NOFORN and REL TO (see below) or NOFORN and EYES ONLY portions, NOFORN takes precedence for the markings at the top and bottom of the page.~~

~~**e. "AUTHORIZED FOR RELEASE TO (REL TO) (name of country (ies)/international organization)".** This marking is used to identify Intelligence Information that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign/international organization indicated.~~

- ~~Paragraph **9-304. Limitation on Dissemination of Classified Intelligence Information.** A contractor is not authorized to further disclose or release classified intelligence information (including release to a subcontractor) without prior written authorization of the releasing agency.~~

- ~~Paragraph **9-305. Safeguarding Classified Intelligence Information.** All classified intelligence information in the contractor's possession shall be safeguarded and controlled according to the provisions of this manual for classified information of the same classification level, with any additional requirements and instructions received from the GCA, and with any specific restrictive markings or limitations that appear on the documents themselves.~~

- ~~Paragraph **9-306. Inquiries.** All inquiries concerning source, acquisition, use, control, or restrictions pertaining to classified intelligence information shall be directed to the providing agency.~~

- Chapter 9, Section 4 (Pages 9-4-1 to 9-4-2):

  - Paragraph 9-402. a. Before a COMSEC account can be established and a contractor may receive or possess COMSEC material accountable to a COR, individuals occupying the positions of FSO, COMSEC ~~custodian~~*Account Manager,* and

alternate COMSEC ~~custodian~~ *Account Manager* must have a final PCL appropriate for the material to be held in the account. COMSEC ~~custodians~~ *Account Managers* and alternate COMSEC ~~custodians~~ *Account Managers* having access to *operational* TOP SECRET keying material marked as ~~containing~~ CRYPTOGRAPHIC (CRYPTO) ~~information~~ must have a final security clearance based upon an SSBI current within five years. This requirement does not apply to contractors using only data transfer devices and seed key.

b. Before disclosure of COMSEC information to a contractor, GCAs must first verify with the CSA that appropriate COMSEC procedures are in place at the contractor facility. If procedures are not in place, the GCA shall provide a written request and justification to the CSA to establish COMSEC procedures and a COMSEC account, if appropriate, at the facility and to conduct the initial COMSEC *or Cryptographic Access* briefings for the FSO and ~~custodians~~ *COMSEC account personnel.*

- Paragraph 9-403. **Establishing a COMSEC Account**

a. When COMSEC material which is accountable to a COR is to be provided, acquired or produced under a contract, the contracting officer shall inform the contractor that a COMSEC account must be established. The contractor shall forward the names of U.S. citizen employees who will serve as the COMSEC ~~Custodian~~ *Account Manager* and Alternate COMSEC ~~Custodian~~ *Account Manager* to the CSA. The CSA shall forward the names of the FSO, COMSEC ~~Custodian~~*Account Manager*, and Alternate ~~Custodian~~ *COMSEC Account Manager, along with a contractual requirement for the establishment of a COMSEC Account (DD Form 254, "Contract Security Classification Specification")* to the appropriate COR, with a copy to the GCA, indicating that the persons have been cleared and COMSEC has been briefed.

b. The COR will then establish the COMSEC account and *will* notify the CSA that the account has been established.

c. An individual may be appointed as the COMSEC ~~custodian~~*Account Manager or Alternate COMSEC Account Manager* for more than one account only when approved by each COR concerned.

- Paragraph 9-404. **9-404. COMSEC Briefing and Debriefing Requirements**

a. All contractor employees who require access to classified COMSEC information in the performance of their duties shall be briefed before access is granted. Depending on the nature of COMSEC access required, either a COMSEC briefing or a Cryptographic Access Briefing will be given. The FSO, the COMSEC

~~Custodian~~*Account Manager*, and the Alternate *COMSEC Account Manager* ~~Custodian~~ shall be briefed by a government representative or their designee. Other contractor employees shall be briefed by the FSO, the COMSEC ~~Custodian, the Alternate Custodian~~*Account personnel*, or other individual designated by the FSO. The purpose of the briefing is to ensure that the contractor understands:

- Paragraph 9-404c. The contractor shall maintain a record of all COMSEC briefings *as specified by the appropriate COR*.

- Paragraph 9-405b. U.S. classified CRYPTO information does not include seed key ~~and~~*or* CCI.

- Paragraph 9-405f. CRYPTO access briefings fully meet the requirements of paragraph ~~9-407~~ *9-405* of this manual for COMSEC briefings.

- Paragraph 9-406. **Destruction and Disposition of COMSEC Material**. The *appropriate* COR shall provide directions to the contractor when accountable COMSEC material is to be destroyed. These directions may be provided in superseding editions of publications or by specific instructions.

- Paragraph 9-408. **Unsolicited Proposals.** Any unsolicited proposal for a COMSEC system, equipment, development, or study that may be submitted by a contractor to a government agency shall be forwarded to the ~~Deputy~~ Director, Information ~~Systems Security~~*Assurance*, NSA, Fort George G. Meade, MD 20755-6000, for review and appropriate follow-up action.

CHAPTER 10, INTERNATIONAL SECURITY REQUIREMENTS

- Chapter 10, Section 3 (Page 10-3-1)

  - Paragraph 10-303b. Duplicate paragraph numbering corrected to paragraph c. 10-303~~b~~*c*. It is the responsibility of the foreign entity that awards the contract to incorporate requirements for the protection and marking of RESTRICTED or "In Confidence" information in the contract. The contractor shall advise the CSA if requirements were not provided by the foreign entity.

  - Paragraph 10-308. **Transfer.** Foreign government information shall be transferred within the U.S. and its territories using the same channels as specified by this ~~m~~*M*anual for U.S. classified information of an equivalent classification, except that non-cleared express overnight carriers shall not be used.

- Chapter 10, Section 4 (Page 10-4-3)

- Paragraph 10-408a & 10-408b: "10-408. Transfers ~~of Technical Data~~ Pursuant to an ITAR Exemption

  a. The contractor shall provide to the DGR valid documentation (i.e., license, Letter of Offer and Acceptance, or agreement) to verify the export authorization for classified technical data *or certain defense articles* to be transferred under an exemption to reference (~~w~~ v). The documentation shall include a copy of the Form DSP-83 associated with the original export authorization.

  b. Classified technical data *or certain defense articles* to be exported pursuant to reference (~~w~~ v) exemptions 125.4(b)(1), 125.4(c), 125.5, 126.4(a), or 126.4(c) shall be supported by a written authorization signed by an Authorized Exemption Official or Exemption Certifying Official who has been appointed by the responsible Principal Disclosure Authority of the GCA. A copy of the authorization shall be provided by the contractor through the CSA to the ~~Office~~ *State Department, Directorate* of Defense Trade Controls *(DDTC)*.

- Chapter 10, Section 7 (Page 10-7-1)
  - Edited Paragraph 10-701. **Classification Levels.** NATO has the following levels of security classification: COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). Another marking, ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and ~~United Kingdom~~ *UK* Atomic information that has been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

- Chapter 10, NEW Section 8, "Transfers of Defense Articles to the United Kingdom without a License or Other Written Authorization" (Pages 10-8-1 through 10-8-2):

- Chapter 10, Section 8, Title edited, "**Transfers of Defense Articles to *AUS or* the ~~United Kingdom~~ *UK* without a License or Other Written Authorization**" (Pages 10-8-1 through 10-8-2):

  - Paragraph **10-800 General.** On June 21, 2007, the U.S. signed the Defense Trade Cooperation Treaty between the Government of the United States of America and the Government of the ~~United Kingdom~~ *UK* of Great Britain and Northern Ireland *(reference (ao)) and on September 5, 2007 between the Government of the United States of America and the Government of AUS (reference (ap))* ~~C~~concerning Defense Trade Cooperation*s* (U.S.-UK Treaty *and U.S.-AUS Treaty, referred to collectively in this Manual as "the Treaties"*). The U.S.-UK Treaty entered into force on April 13, 2012. *The U.S.-AUS Treaty entered into force on May 16, 2013.* The ~~U.S.-U.K~~. Treat~~y~~*ies* provide~~s~~ a comprehensive framework for exports

and transfers to the UK *or AUS* of certain classified and unclassified defense articles without a license or other written authorization. Reference (v) has been amended to implement the ~~U.S.-U.K~~. Treat~~y~~*ies through new exemptions in parts 126.16 and 126.17*. ~~Amendments included a new exemption in~~ Supplement No. 1 to part 126 of reference (v)~~, which~~ identifies those defense articles ~~exempt from the scope of reference (v)~~ *and services that are not eligible for export via Treaty exemptions*. This exemption applies to contractors registered with the ~~State Department, Directorate of Defense Trade Controls (~~DDTC~~)~~, and eligible to export defense articles.

- Paragraph **10-801 Defense Articles.** Defense articles fall under the scope of the ~~U.S.-U.K.~~ Treat~~y~~*ies* when they are in support of:

  a. U.S. and UK *or U.S. and AUS* combined military or counter-terrorism operations;

  b. U.S. and UK *or U.S. and AUS* cooperative security and defense research, development, production, and support programs;

  c. Mutually agreed specific security and defense projects where the Government*s* of the UK *or AUS* is the end-user; or
- Paragraph 10-802.

  a. Classified U.S. Defense Articles shall be marked:

  (1) Treaty with the Government of UK

  CLASSIFICATION LEVEL USML//REL ~~USA AND~~ GBR *AND USA* TREATY COMMUNITY//

  For example, for defense articles classified SECRET, the marking shall be "SECRET USML//REL ~~USA AND~~ GBR *AND USA* TREATY COMMUNITY//"

  (2) Treaty with the Government of AUS

  //CLASSIFICATION LEVEL USML//REL AUS AND USA TREATY COMMUNITY//

  For example, for Defense Articles classified SECRET, the marking will be "//SECRET USML//REL AUS AND USA TREATY COMMUNITY//"

  c. Unclassified U.S. defense articles shall be marked:

(1) ***Treaty with the Government of UK***

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

(2) ***Treaty with the Government of AUS***

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

d. When defense articles are returned from the UK *or AUS* to the U.S., any defense articles marked as RESTRICTED in this manner purely for the purposes of the ~~U.S. U.K.~~ Treat~~y~~*ies* shall be considered to be unclassified and such marking shall be removed.

- Paragraph ***10-803 Notice.*** *The following notice shall be included (e.g., as part of the bill of lading) whenever defense articles are exported in accordance with the provisions of these Treaties and reference (v):*

  These U.S. Munitions List commodities are authorized by the U.S. Government under the U.S.-[AUS or UK, as applicable] Defense Trade Cooperation Treaty for export only to [AUS or UK, as applicable] for use in approved projects, programs or operations by members of the [AUS or UK, as applicable] Community. They may not be retransferred or re-exported or used outside of an approved project, program, or operation, either in their original form or after being incorporated into other end-items, without the prior written approval of the U.S. Department of State.

- Paragraph ***10-804. Labelling***

  a. Defense articles (as defined in section 120.6 of reference (v)) (other than technical data) will be individually labeled with the appropriate identification; or, where such labeling is impracticable (e.g., propellants, chemicals), will be accompanied by documentation (such as contracts or invoices) clearly associating the defense articles with the appropriate markings.

  b. Technical data (as defined in section 120.10 of reference (v)) (including data packages, technical papers, manuals, presentations, specifications, guides and reports), regardless of media or means of transmission (i.e., physical, oral, or electronic), will be individually labeled with the appropriate identification detailed; or, where such labeling is impracticable will be accompanied by documentation (such as contracts or invoices) or oral notification clearly associating the technical data with the appropriate markings.

c. Defense services (as defined in section 120.9 of reference (v)) will be accompanied by documentation (contracts, invoices, shipping bills, or bills of lading) clearly labeled with the appropriate identification.

- Paragraph 10-803 renumbered to 10-805 and edited as follows: ~~**10-803**~~ ***10-805.*** **Transfers.**

  a. All Defense Articles that fall under the scope of the ~~U.S.-U.K.~~ Treat~~y~~*ies* must be transferred from the U.S. point of embarkation through channels approved by both the U.S. and the UK *or the U.S. and AUS, as applicable*.

- Paragraph 10-804 renumbered to 10-806 and edited as follows: ~~**10-804**~~ ***10-806*** **Records.** Contractors shall maintain records of exports, transfers, re-exports, or re-transfers of defense articles subject to the ~~U.S.-U.K.~~ Treat~~y~~*ies* for a ~~period~~ *minimum* of 5 years. Records shall be made available to DSS upon request. The records shall contain the following information required by ~~126.17(l)(1) of~~ *Sections 126.16 and 126.17 of* reference (v)*:*

  f. ~~Reference (v) and j~~*J*ustification for export under the Treat~~y~~*ies*.

  l. All information relating to political contributions, fees, or commissions furnished or obtained, offered, solicited, or agreed upon, as outlined in part*s 126.16(m) or* 126.17(m) of reference (v).

CHAPTER 11, MISCELLANEOUS INFORMATION

- Chapter 11, Section 1 (Page 11-1-1)

  - Paragraph **11-102. Cost**. All costs associated with applying TEMPEST countermeasures, when such countermeasures are imposed upon the contractor by a GCA, shall be recoverable by direct charge to the applicable contract. The GCA should provide TEMPEST shielding and shielded equipment~~s~~ as government-furnished equipment (GFE) when such extreme countermeasures are deemed essential to the protection of the information being processed.

- Chapter 11, Section 2 (Page 11-2-1)

  - Paragraph **11-200. General.** The Department of Defense operates certain activities to assist individuals and organizations in gaining access to scientific and technical information describing planned or on-going research, development, ~~technical and engineering~~ *test, and evaluation* (RDT&E) efforts of the Department of Defense. DTIC is the central point within the Department of Defense for acquiring, storing, retrieving, and disseminating scientific and technical information to support the management and conduct of DoD RDT&E and study programs

APPENDIX A: Cognizant Security Office Information (pages A-1 to A-2)

- Deleted: ~~**Department of Defense** ***DoD***~~

- Edited: *DoD as a CSA, designates DSS as its CSO.* DSS is headquartered in Northern Virginia. The field organization structure consists of four regions. Each region is comprised of Field Offices that employ Industrial Security Representatives *(ISRs)* to provide security oversight, consultation and assistance to over ~~11,000~~ *13,000* contractors. *The DSS* Field Offices *and the ISRs have supporting IS Security Professionals and Counterintelligence personnel, who work with the contractor on NISPOM-related matters. Field offices* are located throughout the United States. Refer to the DSS website (www.dss.mil) for a listing of office locations and areas of responsibility.

- ~~Department of Energy~~ *DOE*

- DOE*, as a CSA,* designates the DOE Field Office Safeguards and Security Divisions~~, listed below,~~ as *its* CSO, Clearance Agency, CVA, Adjudicative Authority, and PCL and FCL databases for ~~their~~ *its* contractors.

- U.S. Department of Energy
  National Nuclear Security Administration Office of Personnel and Facility Clearances
  Pennsylvania & H Street, Kirtland Air Force Base
  Albuquerque, NM 87116
  (505) 845-~~4154~~ *4844*

- U.S. Department of Energy
  Chicago ~~Regional~~ Office*, Bldg. 201*
  9800 South Cass Avenue
  Argonne, IL 60439
  (630) 252-2000 (Operator)

- ~~U.S. Department of Energy~~
  ~~Nevada Operations Office~~
  ~~232 Energy Way~~
  ~~North Las Vegas, NV 89030-4199~~
  ~~(702) 295-1000~~

- ~~With regard to~~ *For* International Affairs and Industrial Security International, the DOE designates *the*:

- ~~Central Intelligence Agency~~ ***CIA***

- ~~The CIA designates the procedure listed below, for~~ *The ODNI designates the CIA as its* ~~CSO, Clearance Agency, CVA, Adjudicative Authority, and PCL and FCL databases for their~~ *its* ~~contractors~~.

- ~~Contact the assigned Contract Officer's Security Representative (COSR) Central Intelligence Agency~~ *Industrial Security Program, Office of Security, CIA,* ~~Washington, DC 20505~~

- The NRC*, as a CSA,* designates *the following* office ~~listed below~~ as ~~the~~ *its* CSO, Adjudicative Authority, International Affairs Office, PCL and FCL databases, and the Office of Industrial Security International for their contractors.

- The NRC designates the offices ~~listed below~~ as the Clearance Agency and Central Verification Agency for ~~their~~ *its* contractors.

APPENDIX C: DEFINITIONS (pages C-1 to C-7)

- **Adverse Information.** Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, ~~or~~ that his or her access to classified information clearly may not be in the interest of national security*, or that the individual constitutes an insider threat.*

- **Approved Access Control Device.** An access control device that meets the requirements of this ~~m~~*M*anual as approved by the FSO.

- **Approved Electronic, Mechanical, or Electro-Mechanical Device.** An electronic, mechanical, or electro-mechanical device that meets the requirements of this ~~m~~*M*anual as approved by the FSO.

- NEW: ***AUS Community.*** *Consists of the Government of Australia entities and Australian non-governmental facilities identified on the DDTC website (http://pmddtc.state.gov/) at the time of export or transfer.*

- NEW: ***Certification.*** *Defined in the Committee on National Security Systems Instruction No. 4009, (reference (aq)).*

- **Closed Area.** An area that meets the requirements of this ~~m~~*M*anual for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

- NEW: ***Counterintelligence.*** *Defined in reference (e).*

- NEW: ***Covered IS.*** *An IS that is owned or operated by or for a cleared defense contractor and that processes, stores, or transmits information created by or for the Department of Defense with respect to which such contractor is required to apply enhanced protection (e.g., classified information).*

- NEW: ***Cybersecurity.*** *Defined in the National Security Presidential Directive-54 (reference (ar)). Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.*

- NEW: ***Cyber Incident.*** *Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an IS or the information residing therein.*

- NEW: **Defense Articles.** Those articles, services, and related technical data, including software, in tangible or intangible form, which are listed on the United States Munitions List (USML) of reference (v), as modified or amended. Defense articles exempt from the scope of §126.17 of reference (v) are identified in Supplement No. 1 to Part 126 of reference (v).

- **Freight Forwarder (Transportation Agent).** Any agent or facility designated to receive, process, and transship U.S. material to foreign recipients. In the context of this ~~m~~*M*anual, an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

- NEW: ***Insider.*** *Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.*

- NEW: ***Insider Threat.*** *The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.*

- NEW: ***Media.*** *Defined in reference (aq).*

- Edited note below: **National of the United States.** A citizen of the United States or a person who, though not a citizen of the United States, owes permanent allegiance to the United States.

- **NOTE:** 8 USC 1101(a)(22)~~, 8 USC 1401, subsection (a)~~ (reference (~~y~~)(x)) lists ~~in paragraphs (1) through (7)~~ categories of persons born in and outside the United States or its possessions who may qualify as nationals of the United States. This subsection should be consulted when doubt exists as to whether or not a person can qualify as a national of the United States.

- **Proscribed Information.**
  a. Top Secret information;

  b. COMSEC information~~, except classified keys used for data transfer~~ *or material, excluding controlled cryptographic items when unkeyed or utilized with unclassified keys*;

- ~~**Special Access Program (**~~**SAP**~~**).**~~ Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A ~~Special Access Program~~ *SAP* can be created or continued only as authorized by a senior agency official delegated such authority pursuant to reference (b).

- **Standard Practice Procedures (SPP).** A document(s) prepared by a contractor that implements the applicable requirements of this ~~m~~*M*anual for the contractor's operations and involvement with classified information at the contractor's facility.

- NEW: ***Transclassified Foreign Nuclear Information (TFNI).*** *Defined in the DOE Order 475.2B (reference (as)).*

- NEW: **UK Community.** Consists of the UK Government entities with facilities and non-governmental facilities identified on the DDTC website (http://www.pmddtc.state.gov/) at the time of export.

- NEW: **Working papers**: Documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention.

New Appendix: ***APPENDIX D: NISPOM Supplement – Security Requirements for SAPs, SCI, IC Compartmented Programs, RD, and FRD*** (pages D-1 to D-4)

- Paragraph ***1. General***. *Given the sensitive nature of the classified information in these categories, the security requirements prescribed in this appendix are in addition to NISPOM standards, and must be applied through specific contract requirements.*

  1.1. The contractor will comply with the security measures reflected in this appendix and other issuances specifically referenced, when applied by the GCA or designee as part of a contract. Acceptance of the contract security measures is a prerequisite to any

negotiations leading to program participation and an area accreditation (e.g., a SCIF or a SAP facility accreditation).

1.2. In some cases, security or sensitive factors of a CSA-created program may require security measures that exceed the standards of this appendix. In such cases, the CSA-imposed higher standards specifically detailed in the contract or conveyed through other applicable directives will be binding on government and contractor participants. In cases of doubt over the specific provisions, the contractor should consult the program security officer and the contracting officer before taking any action or expending program-related funds. In cases of extreme emergency requiring immediate attention, the action taken should protect the government's interest and the security of the program from compromise.

1.3. Every effort will be made to avoid waivers to established standards unless they are in the best interest of the government. In those cases where waivers are deemed necessary, a request will be submitted in accordance with the procedures established by the CSA.

- Paragraph ***2. SAPS***.

*2.1. **DoD SAP Contracts**. Contractors will implement the security requirements for SAPs codified in SAP-related policy, when established by contract, in accordance with applicable statutes, Executive orders, CSA directives, instructions, manuals, regulations, standards, memorandums, and other SAP security related policy documents.*

*2.2. **Non-DoD SAPS.** Contractors performing on SAP contracts issued by other than DoD GCAs, will implement SAP protection requirements imposed in their contracts. These requirements may be from, but are not limited to, statutes, Executive orders, CSA directives, instructions, manuals, regulations, standards, memorandums, and other SAP security related policy documents.*

- Paragraph ***3. Alternative Compensatory Control Measures (ACCM).*** *Contractors may participate in ACCMs, or be directed to participate, only when such access and the associated security plan are identified in DD Form 254. Care must be taken to ensure identification of the security plan does not disclose ACCM-protected data.*

*3.1. **ACCM Contracts**. DoD contractors will implement the security requirements for ACCMs, when established by contract, in accordance with applicable statutes, Executive orders, CSA directives, instructions, manuals, regulations, standards, memorandums, and other SAP security related policy documents.*

*3.2. **Non-DoD with ACCMs.** Contractors performing on ACCM contracts issued by other than DoD GCAs, will implement ACCM protection requirements imposed in their contracts.*

- Paragraph ***4. IC Compartmented Programs***

  4.1. This section encompasses SCI and IC SAPs (collectively referred to in this issuance as "Controlled Access Programs (CAPs)") requiring compartmentation and enhanced protection when the vulnerability of, or threat to, specific information is exceptional and normal standards, criteria, processes, and accesses are insufficient to protect such information from unauthorized disclosure.

  4.2. Contractors will implement the security requirements for CAPs in accordance with applicable CAP-related issuances, when established by contract. These issuances include all DNI security-related policy documents that may pertain to the protection of CAP and CAP-related information.

- Paragraph ***5. RD, FRD, and TFNI***

  5.1. ***General****. This section describes requirements for nuclear-related information designated RD, FRD, or TFNI in accordance with reference (c). Part 1045 of Title 10, CFR (reference (p)) contains the requirements for classification and declassification of RD and FRD. Additional handling and protection requirements are included in DOE policy.*

  5.1.1 Control and distribution of RD will be sufficient to assure common defense and security. Weapon data is always RD or FRD, specifically that portion concerning design, manufacture, or use of atomic weapons. RD and FRD categories are distinguished from the NSI category, which is governed in accordance with reference (b). It is necessary to differentiate between the handling of this information and NSI because of its direct relationship to our nation's nuclear deterrent.

  5.1.2 Principal authority for setting requirements for classifying, accessing, handling, and securing and protecting RD is entrusted to the Secretary of Energy.

  5.1.3 Some access requirements for RD and FRD exceed the requirements for NSI. It is important to note that due to the unique national security implications of RD and FRD, and to facilitate maintaining consistency of codified requirement, they are not repeated in the baseline NISPOM, but may be applied through specific contract requirements.

  5.1.4 When RD is transclassified to TFNI, it is safeguarded as NSI. Such information will be labeled as TFNI. The label TFNI will be included on documents to indicate it is exempt from automatic declassification as specified in part 1045 of reference (p) and references (c), (b,) and (z).

  5.2. ***Unauthorized Disclosures****. Contractors will report all unauthorized disclosures involving RD, FRD and TFNI information to the CSA.*

*5.3. **International Requirements**. Reference (c) provides for a program of international cooperation to promote common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit. Pursuant to section 123 of reference (c), information controlled by reference (c) may be shared with another nation only under the terms of an agreement for cooperation. The disclosure by a contractor of RD and FRD will not be permitted until an agreement is signed by the United States and participating governments, and disclosure guidance and security arrangements are established. RD and FRD will not be transmitted to a foreign national or regional defense organization unless such action is approved and undertaken under an agreement for cooperation between the U.S. and the cooperating entity and supporting statutory determinations, as prescribed in reference (c).*

*5.4. **Personnel Security Clearances and Access**. Only DOE, NRC, DoD, and NASA can grant access to RD and FRD that is under their cognizance. Access to RD and FRD must be granted in accordance with reference(c). Baseline requirements for access to RD and FRD are codified in specific DoD, DOE, NRC, and NASA directives and regulations. In addition, need-to-know and other restrictions on access may apply.*

*5.5. **Classification and Declassification***

5.5.1 All persons with access to RD and FRD must be trained on the authorities required to classify and declassify RD and FRD information and documents and on handling procedures in accordance with parts 1045 and 1016 of reference (p).

5.5.2 Any person who believes he or she has information that may be RD or FRD must submit it to an RD classifier for evaluation.

5.5.3 Only RD classifiers may classify documents containing RD or FRD. RD classifiers must be trained on the procedures for classifying, declassifying, marking, and handling RD, or FRD and documents in accordance with part 1045 of reference (p).

5.5.4 RD classifiers will use classification guides as the primary basis for classifying documents containing RD, FRD, and TFNI.

5.5.5. RD classifiers cannot declassify a document marked as containing RD, FRD, or TFNI. Declassification includes redacting RD, FRD, and TFNI portions from a document and removing RD, FRD, and TFNI markings from documents. RD documents must be sent to designated individuals in DOE. FRD documents must be sent to designated individuals in DOE or appropriate officials in DoD.

5.5.6 RD and FRD documents must include:

5.5.6.1 The RD classifier's name and position or title.

5.5.6.2 The classification guide or source document (by title and date) used to classify the document.

5.5.7 No date or event for automatic declassification ever applies to RD, FRD or TFNI documents, even if they contain classified NSI. RD, FRD or TFNI documents remain classified until a positive action by a designated DOE official (for RD, FRD or TFNI) or an appropriate DoD official (for FRD) is taken to declassify them.

5.5.8 Any RD or FRD document intended for public release in an RD or FRD subject area must be reviewed for classification by the appropriate DOE organization (for RD or TFNI) or the appropriate DOE or DoD organization (for FRD) prior to its release.

5.5.9 Consult DOE Manual 205.1B (reference (at)) for additional information and requirements. Contact the DOE Office of Classification at outreach@hq.doe.gov or at (301) 903-7567 for additional information concerning the classification and declassification of RD and FRD.

*5.6. **Automatic declassification**. Documents containing TFNI are excluded from the automatic declassification provisions of part 1045 of reference (p) until the TFNI designation is properly removed by DOE. When DOE determines that a TFNI designation may be removed, any remaining information classified must be referred to the appropriate agency in accordance with reference (c) and part 1045 of reference (p).*

*5.7. **Challenges to RD, FRD and TFNI Classification**. Any contractor employee who believes that an RD, FRD, or TFNI document is classified improperly or unnecessarily may challenge that classification following the procedures established by the GCA.*

*5.8. **Comingling**. Comingling of RD, FRD, and TFNI with information classified, in accordance with reference (b), in the same document should be avoided to the greatest degree possible. When mixing this information cannot be avoided, the protection requirements of references (b) and (z), as well as Part 2003 of reference (z) must be met.*

*5.9. **Marking RD and FRD**. RD and FRD, in addition to any traditional NSI classification markings, will include RD category admonishment information on the first page, RD or FRD marked at the top and bottom of each interior page containing it, and notation of Sigma information. These markings may appear on any classification level (CONFIDENTIAL, SECRET, or TOP SECRET) documents. Weapon data documents being sent outside the weapons complex will bear the marking NUCLEAR WEAPON DATA, or CNWDI, as appropriate. Further information regarding these requirements can be found at https://www.directives.doe.gov/ and www.nnsa.energy.gov or, by e-mail to Security.Directives@hq.doe.gov.*

*5.10. **Protection of RD and FRD**. Most of the protection requirements for RD and FRD are similar to NSI and are based on the classification level; however, there are some specific protection requirements for certain Sigma information that may be applied through specific contract requirements by the GCA. These range from distribution limitations through the limitation of access to specifically authorized individuals to specific storage requirements, including the requirement for intrusion detection systems, and additional accountability records (i.e., Sigmas 14, 15, and 20).*

5.10.1. Any DOE contractor that violates a classified information security requirement may be subject to a civil penalty under the provisions of part 824 of reference (p).

5.10.2. Certification is required for individuals authorized access to specific Sigmas, as appropriate. Address questions regarding these requirements to Security.Directives@hq.doe.gov.

5.10.3. Storage and distribution requirements are determined by the classification level, category, and Sigma. All RD documents do not require a Sigma designation. Storage and distribution requirements will be dependent only on classification level and category.

*5.11. **Accountability**. In addition to TS information, some S/RD information is considered accountable (e.g., specific Sigma 14, 15, and 20 documents.) Each weapon data control point will keep a record of transactions involving Secret weapon data documents under its jurisdiction including origination, receipt, transmission, current custodian, reproduction, change of classification, declassification, and destruction.*

*5.12. **Cyber**. Classified databases, systems and networks containing RD and FRD are protected under the requirements developed and distributed by the DOE Office of the Chief Information Officer.*

*5.13. **References**. The following may not have been previously referenced, but are some of the primary directives that cover RD and FRD. Information regarding copies of DOE Security Directives may be requested via e-mail at: Security.Directives@hq.doe.gov.*

*5.13.1 **Reference (at)**. Reference (at) provides baseline requirements and controls for the graded protection of the confidentiality, integrity, and availability of classified information and IS used or operated by the DOE, contractors, and any other organization on behalf of DOE, including the National Nuclear Security Administration.*

*5.13.2 **DOE Order 452.7 (Reference (au))**. Reference (au) establishes a general process and provides direction for controlling access to and distributing Sigma 14 and 15 nuclear weapon data at the DOE. It supplements*

DOE Order 452.4B (reference (av)), which establishes DOE requirements and responsibilities to prevent the deliberate unauthorized use of U.S. nuclear explosives and nuclear weapons.

5.13.3 ***DOE Order 473.3 (Reference (aw))****. Reference (aw) establishes requirements for the physical protection of safeguards and security interests. Copies of certain sections of reference (aw) (e.g., Attachment 3, Annex 1, Safeguards and Security Alarm Management System, which contains Unclassified Controlled Nuclear Information) are only available, by request, from Security.Directives@hq.doe.gov or, by phone at (301) 903-1159.*

5.13.4 ***DOE Order 471.6 (Reference (ax))****. Reference (ax) establishes security requirements for the protection and control of matter required to be classified or controlled by statutes, regulations, or DOE directives.*

5.13.5 ***DOE Order 483.1-1A (Reference ay).*** *Reference (ay) provides policy, requirements, and responsibilities for the oversight, management and administration of Cooperative Research and Development Agreement activities at DOE facilities.*