DCMA Manual 3301-08

Information Security

Office of Primary Responsibility	**Integrating Capability – Agency Mission Assurance**
Effective:	January 21, 2019
Releasability:	Cleared for public release
Implements:	DCMA-INST 3301, "Agency Mission Assurance," May 14, 2018
Incorporates and Cancels:	DCMA-INST 552, “Information Security,” May 8, 2017
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.dcma.mil/sites/policy/MA/SitePages/3301-08r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: This issuance assigns responsibilities and establishes processes and procedures for implementing the DoD Information Security Program in compliance with DoD Instruction 5200.1, higher level policies, other laws, and Executive Orders in accord with the authority in DoD Directive 5105.64 and DCMA Instruction 3301.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA activities and personnel unless higher-level regulations, policy, guidance, or agreements take precedence.

1.2. POLICY. It is DCMA policy to:

a. Identify, classify, downgrade, declassify, mark, protect, and dispose of classified and controlled unclassified information (CUI) consistent with national and DoD policy.

b. Protect information by delegating authority to the lowest levels possible, encouraging and advocating the use of risk management principles, focusing on identifying and protecting only information requiring protection, integrating security procedures into Agency business processes so they become transparent, and ensuring all personnel understand their security-related roles and responsibilities.

c. Establish all DCMA personnel are personally responsible for protecting classified information and CUI under their custody and control. All officials within DCMA who hold command, management, or supervisory positions have specific, non-delegable responsibility for the quality of implementation and management of the Information Security (INFOSEC) Program within their areas of responsibility.

d. Execute this Manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DCMA. The DCMA Director will:

a. Ensure the establishment and resourcing of a comprehensive INFOSEC Program complying with the requirements established in DoD Instruction (DoDI) 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," and other applicable references.

b. Designate a senior agency official (SAO) with responsibility for the overarching management and oversight of the INFOSEC Program.

c. Serve as the DCMA original classification authority (OCA).

2.2. COMPONENT HEADS AND CONTRACT MANAGEMENT OFFICE (CMO) COMMANDERS/DIRECTORS. The Component Heads and CMO Commanders/Directors will:

a. Work with the supporting Regional INFOSEC Specialist (RIS) to develop and maintain a site-specific facility security plan (FSP) addressing INFOSEC requirements.

b. Ensure assigned personnel complete required INFOSEC training and comply with the provisions of the DCMA INFOSEC Program.

c. Designate in writing an organizational security representative responsible for the day-to-day oversight and management of the organization's INFOSEC Program.

d. Report actual and/or suspected security incidents involving classified information or CUI to the DCMA INFOSEC team.

e. Following the identification of security incidents involving classified information or CUI, appoint an individual to conduct a preliminary inquiry or formal investigation (as necessary) to identify and document the relative facts and circumstances surrounding the incident.

2.3. EXECUTIVE DIRECTOR, SPECIAL PROGRAMS DIRECTORATE (DCMAS). The Executive Director, DCMAS will:

a. Establish DCMA-specific Special Access Program (SAP) policy and processes ensuring implementation of applicable higher-level policies.

b. Serve as the senior intelligence officer (SIO) responsible for the agency sensitive compartmented information (SCI) security program per DoDM 5105.21, Volume 1, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security," DoDM 5105.21, Volume 2, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," and DoDM 5105.21, Volume 3, "Sensitive

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

c. Appoint a special security officer (SSO) responsible for coordinating sensitive compartmented information facility (SCIF) accreditation and management of DCMA SCIFs.

d. Appoint a DCMAS program security officer (PSO) responsible for the administration of security policies and requirements.

e. Ensure facilities constructed for SAP and SCI operations meet applicable standards.

f. Ensure all personnel assigned to DCMAS complete required SAP and SCI training, briefings, and other requirements.

2.4. OFFICE OF GENERAL COUNSEL (OGC). The OGC will provide legal assistance and advice in support of the INFOSEC Program.

2.5. DIRECTOR, SECURITY AND COUNTERINTELLIGENCE (DSCI). The DSCI will:

a. Serve as the SAO responsible for the development, implementation, and oversight of the INFOSEC Program.

b. Appoint a PM to manage the INFOSEC Program.

c. Ensure the INFOSEC Program is integrated with other security-related programs in support of an overarching security/mission assurance construct.

d. Advocate for and allocate resources in support of the INFOSEC Program.

2.6. INFOSEC PROGRAM MANAGER (ISPM). The ISPM will:

a. Develop and manage an effective INFOSEC Program that complies with the prescribing directives.

b. Develop and maintain Agency-level INFOSEC policy, training, and supporting tools that ensures compliance with the prescribing directives are tailored to the DCMA mission.

c. Identify and manage resources assigned to support the INFOSEC Program.

d. Maintain close liaison and coordination with all INFOSEC Program stakeholders.

e. Develop and implement an effective INFOSEC assessment program.

f. Implement other requirements listed herein.

2.7. INFOSEC PROGRAM TEAM LEAD (IPTL). The IPTL will:

a. Report to the ISPM and manage all operational aspects of the INFOSEC Program.

b. Execute INFOSEC programs and policies.

c. Implement and track required INFOSEC training.

d. Consolidate and report INFOSEC Program resource requirements.

e. Administer inquiries and investigations associated with security incidents involving classified information or CUI.

f. Implement other requirements listed herein or as directed by the ISPM.

2.8. REGIONAL INFOSEC SPECIALISTS (RIS). The RIS will:

a. Report to the IPTL.

b. Provide INFOSEC support by maintaining coordination, and INFOSEC guidance and assistance to Commanders, Directors, and Security Representatives within assigned region.

c. Track inquiries or investigations associated with security incidents involving classified information or CUI.

d. Schedule and conduct, prepare and distribute INFOSEC-related assistance visit reports.

e. Track recommendations following assessments through mitigation or remediation.

f. Schedule and deliver INFOSEC training.

2.9. SPECIAL SECURITY OFFICER (SSO). The SSO must:

a. Administer the receipt, control, and accountability of SCI and oversee SCI security functions for subordinate SCIFs.

b. Supervise the special security office and administer the SCI security program to include SCI security oversight for other SCIFs under the organization’s security cognizance.

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

d. Ensure SCI is properly accounted for, controlled, transmitted, transported, packaged, destroyed, and safeguarded.

2.10. SECURITY REPRESENTATIVES. Security representatives will:

a. Provide day-to-day administrative INFOSEC support to the assigned organization.

b. Coordinate INFOSEC related issues, questions, or concerns with the responsible RIS.

c. Coordinate INFOSEC assessment and self-assessment requirements.

d. Report INFOSEC incidents to the DCMA Security INFOSEC staff while taking the necessary actions to protect the applicable information.

2.11. DCMA PERSONNEL. DCMA personnel will:

a. Complete INFOSEC training as documented in Section 9 of this Manual.

b. Promptly report actual or suspected INFOSEC incidents or violations to management, the responsible RIS, or to the IPTL.

c. Protect classified information and CUI under their control.

d. Observe and adhere to classification determinations made by OCAs.

e. Properly mark all materials where a derivative classification decision was rendered in accordance with of DoDM 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," Enclosure 3.

f. Take reasonable steps, including consulting appropriate security classification guidance and/or requesting assistance from the appropriate OCA, to resolve questions or conflicts regarding classification decisions and handling instructions.

g. Apply appropriate distribution statements to all technical documents created to denote the extent to which they are available for distribution, release, and dissemination in accordance with DoDD 5230.24, "Distribution Statements on Technical Documents."

SECTION 3: PROGRAM CONSTRUCT

3.1. GENERAL. In accordance with DoDM 5200.01, Volumes 1-4, "DoD Information Security Program," the DCMA INFOSEC Program is established in three levels (strategic, operational, and tactical) for program implementation throughout the Agency. Responsibilities within each descending level vary according to specific tasks and authorities to implement and execute the program.

3.2. LEVEL III INFOSEC PROGRAM.

a. The Level III INFOSEC Program is established at the strategic (Agency) level and focuses on overall program development, management, and implementation. This level is primarily responsible for policy and program development, implementation, and Agency-level oversight.

b. The DCMA Information Security (INFOSEC) PM is responsible for Level III program management and execution.

3.3. LEVEL II INFOSEC PROGRAM.

a. The Level II INFOSEC Program is established at the operational level and focuses on operational support to the various components by specifically trained and experienced security specialists. This level is responsible for assisting organizations in developing organizational-specific INFOSEC plans and procedures, performing INFOSEC reviews of materials intended for public disclosure, conducting INFOSEC assessments and surveys, and providing other INFOSEC support activities.

b. The DCMA Security INFOSEC Team, organizationally structured within the Headquarters Security Division, is responsible for Level II program implementation.

3.4. LEVEL I INFOSEC PROGRAM.

a. This is the tactical level of INFOSEC Program implementation and resides within the Components and Primary CMO Headquarters. Activities below this level is not required to develop a separate INFOSEC Program from their parent organization; however, programs may be established below the cited level should the responsible Commander/Director determine the mission of a particular subordinate organization warrants enhanced INFOSEC safeguards.

b. This level of INFOSEC program implementation is primarily responsible for applying DoD and Agency level INFOSEC policy, developing organizational-specific INFOSEC plans and procedures, and practicing effective information protection safeguards.

c. The designated organizational security representative, with direct support from the responsible RIS, are responsible for Level I program implementation.

SECTION 4: CLASSIFYING INFORMATION

4.1 . GENERAL.

a. Information will be classified only when necessary and in the interest of national security. Classified information will be downgraded or declassified as soon as is consistent with national security and with the approval of the responsible OCA.

b. Classification will be applied only to information owned by, produced by or for, or is under the control of the U.S. Government. Information may be considered for classification only if its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security, and the information concerns one of the categories specified in Section 1.4 of Executive Order (E.O.) 13526, "Classified National Security Information":

- Military plans, weapon systems, or operations (subsection 1.4(a))
- Foreign government information (FGI) (subsection 1.4(b))
- Intelligence activities (including covert action), intelligence sources or methods, or cryptology (subsection 1.4(c))
- Foreign relations or foreign activities of the United States, including confidential sources (subsection 1.4(d))
- Scientific, technological, or economic matters relating to the national security (subsection 1.4(e))
- U.S. Government programs for safeguarding nuclear materials or facilities (subsection 1.4(f))
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security (subsection 1.4(g))
- The development, production, or use of weapons of mass destruction (subsection 1.4(h))

4.2. CLASSIFICATION PROHIBITIONS.

a. Information may not be classified, continued to be maintained as classified, or fail to be declassified in order to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection in the interests of the national security

b. Basic scientific research and its results may not be classified unless clearly related to national security.

4.3. LEVELS OF CLASSIFICATION.

a. Information identified as requiring protection against unauthorized disclosure in the interest of national security will be classified top secret, secret, or confidential. No other terms will be used to identify U.S. classified information except as otherwise provided by statute.

b. Top Secret will be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

c. Secret will be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.

d. Confidential will be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.

4.4. ORIGINAL CLASSIFICATION.

a. Original classification is the initial decision that an item of information could reasonably be expected to cause identifiable or describable damage to the national security if subjected to unauthorized disclosure and requires protection in the interest of national security.

b. The Director is the sole OCA within DCMA for the classification of DCMA owned or generated information. In accordance with Assistant Secretary of Defense (ASD) Memorandum, "Granting of Original Classification Authority," this authority is limited to secret and confidential original classification decisions. The Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) reserves authority for top-secret OCA decisions.

c. Persons identifying information 0they believe requires protection to prevent damage to the national security will ensure the information is protected at the level of suspected classification. The individual identifying the information will contact DCMA Security and request assistance in preparing an original classification decision package for review by the OCA. Requests for classification decision determinations will be forwarded to DCMA Security INFOSEC Team as soon as possible but not later than 30 days from the date the information was originally identified.

(1) Original classification decision packages will be prepared in an action memorandum format in accordance with the DCMA Manual (DCMA-MAN) 4501-02, "Correspondence Program." The ISPM will assist the requestor in the preparation of the package. The requestor is responsible for documenting the following requirements:

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

(b) The information falls within one or more of the categories of information listed in Paragraph 4.1.

(c) Determine if the information has already been classified by another OCA.

(d) Determine classification guidance is not already available in the form of security classification guides (SCGs), plans, or other memorandums. Within the DoD, the majority of existing classification guidance is indexed and promulgated via the Defense Technical Information Center (DTIC) website.

(e) Additional supporting documentation related to the suspected information deemed necessary to help in the classification decision process.

(2) Upon receipt of the decision package, the ISPM will determine the appropriate method to transmit the information to the OCA for review and decision. When appropriate, the ISPM will advise and assist the OCA with ensuring all statutory and DoD policy requirements are met.

(3) The OCA will conduct the original classification review and render a classification decision within 30 days of receipt of the package. The OCA will communicate the decision to the ISPM. The DCMA Security INFOSEC Team will notify the requestor of the classification decision rendered by the OCA.

(4) All documentation produced during the original classification decision process will be filed permanently within the DCMA Security INFOSEC Team section.

4.5. DERIVATIVE CLASSIFICATION.

a. Derivative classification is the process of incorporating, paraphrasing, restating, or generating in new form information already classified and marking the newly developed material consistent with the classification markings applied to the source information (this includes documents, electronic mail (e-mail), presentations, photographs, charts, spreadsheets, facsimiles (FAX), etc.). Derivative classification includes the classification determination of information based on classification guidance (e.g., a classification guide). Duplication or reproduction (copying) of existing products containing classified information is not considered derivative classification.

b. Personnel who generate or produce items containing classified information derived from originally classified sources will ensure all derivative classifications are applied in accordance with DoDM 5200.01, Volume 1, Enclosure 4. No individual or specific delegation of authority is required to derivatively classify information within a product. The individual who signs or approves derivatively classified products has principal responsibility to ensure the derivative classification is conducted appropriately. Derivative classifiers will:

(1) Observe and respect the classification determinations made by OCAs. If derivative classifiers believe information to be improperly classified, they will take the actions outlined in DoDM 5200.01, Volume 2, Enclosure 4.

(2) Mark classified information in accordance with DoDM 5200.01, Volume 2.

(3) Use only authorized sources for classification guidance (e.g., security classification guides, memorandums, DoD publications, and other forms of classification guidance issued by an OCA).

(4) Ensure classification markings are taken directly from the source documents or materials. Experience or general knowledge will not be used for classification determinations.

(5) Use caution when paraphrasing or restating information extracted from a classified source. Paraphrasing or restating information may change the need or level of classification.

(6) Take reasonable steps, including consulting appropriate security classification guidance and/or requesting assistance from the appropriate RIS or OCA, to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification.

(7) Ensure the identity of the derivative classifier is identified on the new derivatively classified document within the classification authority block as required.

(8) When derivative classification based on multiple sources (e.g., more than one SCG, classified source, or combination thereof) is used, the derivative classifier will compile a list of the sources used. The multiple source list will be included or attached at the end of the derivatively classified product.

c. Derivative Classification Reporting. Commanders or Directors will report derivative classification decisions in accordance with Agency tasking requirements. These reporting processes support Agency-level reporting requirements to the Office of the Under Secretary of Defense for Intelligence (OUSD(I)).

4.6. DURATION OF CLASSIFICATION.

a. When information is classified, a determination must be made regarding how long the information is to be protected (i.e., when the information will lose its sensitivity and no longer merit or qualify for classification). This is an essential part of the classification process. The OCA must determine during the original classification decision process the duration for which information is to be classified. This determination will be contained in the security classification guidance developed at the time of classification decision.

b. For derivatively classified information, the derivative classifier must ensure the most restrictive declassification, destruction, or downgrading instruction (i.e., the one that specifies the longest duration of classification) is carried forward from security classification guidance provided by the OCA. Specific guidance on determining the most restrictive instruction is provided in DoDM 5200.01, Volume 1, Enclosure 4.

4.7. COMPILATION OF INFORMATION.

a. Individual portions of unclassified information (or information classified at a lower level) may become classified (or classified at a higher level) if the compiled information reveals an additional association or relationship meeting the following conditions:

- Qualifies for classification pursuant to Paragraphs 4.1 and 4.3. of this Manual.
- Is not otherwise revealed by the individual elements of the information.

b. Personnel supporting contracts covered by a DD Form 254 "Contract Security Classification Specification," must be cognizant of the security classification guidance cited in the DD Form 254 to ensure compilation of unclassified information does not reveal classified aspects of the contract. If after review of applicable security classification guidance there are still concerns as to the classification of the information, the individual identified in block 16 of the DD Form 254 will be contacted for clarification.

4.8. UNAUTHORIZED PUBLIC RELEASE OF CLASSIFIED INFORMATION.

a. Classified information released to the public without proper authority (e.g., media leak, data spill, etc.) is classified until a proper classification determination is made by the responsible OCA. DCMA personnel will not publicly acknowledge the release of classified information and must not make any statement or comment confirming the accuracy of or verifying the classification of information subject to unauthorized public release.

b. Incidents involving the unauthorized public release of classified information will be promptly reported to the ISPM for action and further reporting to OUSD(I) in accordance with DoDM 5200.01, Volume 3, Enclosure 6 and Section 10 of this Manual. Refer to DCMA-INST 1091, "Special Access Security," concerning unauthorized release of SAP information.

c. Upon notification of an unauthorized public release of information, the ISPM will ensure an inquiry or investigation into the incident is promptly initiated. In addition, a damage assessment will be initiated by the OCA and information owner to determine the effects of the information release to national security and actions required to mitigate the situation.

d. During the course of the damage assessment, should the responsible OCA determine the affected information will remain classified, the OCA (or designated representative) will notify all known holders of the information and provide marking guidance in the event the information was not previously marked or was marked incorrectly.

4.9. PROHIBITION TO AFFECTING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION FOR PROTECTED DISCLOSURE.

a. Any officer or employee of DCMA who has authority to take, direct others to take, recommend, or approve any action affecting an employee's eligibility for access to classified information will not, with respect to such authority, take or fail to take, or threaten to take or fail to take, any action affecting an employee's eligibility for access to classified information as a reprisal for a Protected Disclosure as provided in Presidential Policy Directive-19, "Protecting Whistleblowers with Access to Classified Information."

b. This prohibition applies to persons serving in the Intelligence Community as set forth in E.O. 12333, "United States Intelligence Activities," or to other persons with eligibility for access to classified information who can effectively report waste, fraud, and abuse while protecting classified national security information.

4.10. CHALLENGES TO CLASSIFICATION.

a. General. Under E.O. 13526, all classification decisions are subject to challenge. An individual may challenge classification decisions under the authority of E.O. 13526 if he or she has a substantial reason to believe the classified information in question is improperly or unnecessarily classified. Informal or formal challenges may be submitted in accordance with the guidance identified in paragraphs 4.10.a.(1) and 4.10.a.(2) of this Manual.

(1) Informal Challenges. Informal challenges will be initiated by contacting the responsible RIS directly or by sending an e-mail (containing only unclassified information) to dcma.lee.hq.list.infosec@mail.mil. All informal challenges will include identification of the specific information challenged, contact information of the challenger, and justification for the challenge.

(2) Formal Challenges. Personnel submitting a formal challenge to a classification will submit the challenge in writing in memorandum format. Formal challenges will contain the challenger's contact information (name, official address, telephone number, and e-mail address), the specific document(s) and paragraph(s) challenged, a justification for the challenge, the classification authority, and cite the established DoD policy which contradicts the existing classification. The challenger will submit the challenge to the DCMA Security INFOSEC team at dcma.lee.hq.list.infosec@mail.mil for evaluation and/or action.

b. Classification Challenge Process.

(1) Upon receipt of a challenge, the ISPM will record the request and coordinate with the applicable OCA to obtain a proper classification determination.

(2) Upon the receipt of the classification determination, the ISPM will notify the challenger of the OCA's decision and identify to which official an appeal may be directed.

4.11. DECLASSIFICATION AND CHANGES TO CLASSIFICATION.

a. Pursuant to DoDM 5200.01, Volume 1, Enclosure 4, information will remain classified only as long as the following conditions are met:

- It is in the best interest of national security to maintain the information's classification
- Continued classification is in accordance with E.O. 13526

b. Persons having reason to believe the public interest in the disclosure of classified information outweighs the need for continued classification may refer the matter to the ISPM. The ISPM will contact the appropriate OCA and coordinate classification determinations.

c. When OCA classification determinations are rendered, the ISPM will ensure any change in marking will be conducted in accordance with DoDM 5200.01, Volume 2, Enclosure 3. Any additional security classification guidance issued by the OCA will be implemented.

4.12. SECURITY CLASSIFICATION GUIDES (SCGs).

a. General.

(1) SCGs provide written, standardized guidance for the classification of information issued by an authorized OCA applicable to a specific program, technology, command, or operation. SCGs identify the specific elements of information regarding a subject that must be classified and establish the level and duration of classification for each element. DCMA personnel with access to or using classified information will ensure familiarity with applicable SCGs to protect information entrusted into their care.

(2) There are two basic types of SCGs: technical or program SCGs and operational or command SCGs.

(a) Technical or program SCGs provide classification guidance relative to a specific program or technology. An example of a technical or program SCG would be the MQ-1/MQ-9 Predator SCG.

(b) Operational or command SCGs provide classification guidance relative to a specific command or operation. An example of an operational or command SCG is "Operation Enduring Freedom SCG" or the "Headquarters United States Central Command SCG."

(c) Typical SCGs contain the following elements:

1. Identification of specific items or elements of information to be protected.

2. The specific classification assigned to each item or element of information.

3. A concise reason for classifying each item, element, or category of information and cite the applicable classification category(s).

4. The declassification instructions for each item or element of classified information, including citation of any approved automatic declassification exemption category.

b. Obtaining the Appropriate SCG.

(1) To identify the appropriate SCG, first identify the specific technology, program, command, or operation. If working with a contract, review the contract's list of attachments to

determine if a DD Form 254 is attached. If attached, review block 13 of the DD Form 254 to determine security classification guidance or block 16 for the responsible party that signed the DD Form 254. Review the H-Clause of the contract, in the event security guidance is also contained within the H-Clause section. If a DD Form 254 is not available, contact the responsible RIS for assistance.

(2) Once the applicable SCG is identified, copies may be obtained from various sources:

- DTIC Online Access Controlled (DOAC)
- The responsible program office
- The responsible contractor
- INTELINK (INTELINK is applicable to the secure internet protocol router network (SIPRNet))

c. Using an SCG. To use an SCG, perform the following steps:

(1) Step 1. Review the SCG in detail to understand the specific guidance contained therein.

(2) Step 2. Identify the specific items or elements of information in question.

(3) Step 3. Identify the specific classification assigned to each item or element of information.

(4) Step 4. Identify the concise reason for classifying each item, element, or category of information and applicable classification category(ies).

(5) Step 5. Identify the classification instructions for each item or element of information, including citation of the approved automatic declassification exemption category.

(6) Step 6. Review the remarks section to identify any additional information needed to render a classification determination.

(7) Step 7. Properly mark the items containing the classified information. Section 5 of this Instruction contains guidance for properly marking classified materials.

SECTION 5: MARKING INFORMATION

5.1. GENERAL.

a. Items (documents, electronic media, Web pages, etc.), containing classified information and CUI must be properly marked. Markings are the principal means of informing holders of the presence of classified information or CUI, the information's classification level, and specific protection or handling requirements. All items containing classified information and CUI must be marked to show the information's highest classification level.

b. All items containing classified and CUI will be clearly identified by applying proper markings, designations, or electronic labeling. If physical marking of the medium is not possible, appropriate markings will be applied by some other means.

c. Items containing information designated at more than one level of classification will bear the highest or more stringent level of classification as the overall or banner marking.. Markings, designations, and electronic labeling will be conspicuous, immediately apparent, and will:

(1) Alert holders to the presence of classified information or CUI.

(2) Identify, as specifically as possible, the exact information requiring protection and the level of protection required.

(3) Give information on the source(s) of and reasons for classification of the material.

(4) Identify the office of origin and document originator applying the classification markings.

(5) Provide guidance on information sharing and warn holders of special access, dissemination control, or safeguarding requirements.

(6) Provide guidance on downgrading and declassification for classified material.

5.2. MARKING CLASSIFIED INFORMATION.

a. The individual creating or producing an item containing classified information or CUI is responsible for ensuring proper markings are applied. DCMA personnel using the derivative classification process will refer to the source document(s), SCGs, or other classification guidance issued by an OCA when determining the markings to apply to products containing classified information.

b. DCMA personnel will ensure the required four basic marking components are applied when marking products containing classified information:

(1) Apply a Banner (Overall marking) Line. Banner lines are located at the top and bottom of each classified document and will identify the highest level of classified information (confidential, secret, or top secret) contained in the item.

(2) Apply Portion Markings. Portion markings identify the specific classified information in the product and levels of classification. These markings precede all subjects, Paragraphs, subparagraphs, and bullets.

(3) Identify the Office of Origin and Date Produced. This line will identify the person and specific DCMA office of origin producing the classified document or product, and the date of production. Provide sufficient information to allow for the identification the originating DCMA office should issues or classification questions arise.

(4) Apply the Classification Authority Block. The title page or first page of classified document or product will include a classification authority block consisting of required elements (classified by, derived from, and declassify, downgrade, or destruction information). Classification Authority Blocks applied to electronic mail, messages, web pages, or other venues may consist of a single line of text.

(a) Classified By Line. List name and position title or personal identifier of the OCA or derivative classifier and include the component and office of origin on the classified by line.

(b) Reason (Original Classification) or Derived From Line (Derivative Classification). OCA's or derivative classifiers must show the authority from which information is considered classified.

1. OCA's must include a Reason Line for classifying information by citing the category specified in Section 1.4 of E.O. 13526.

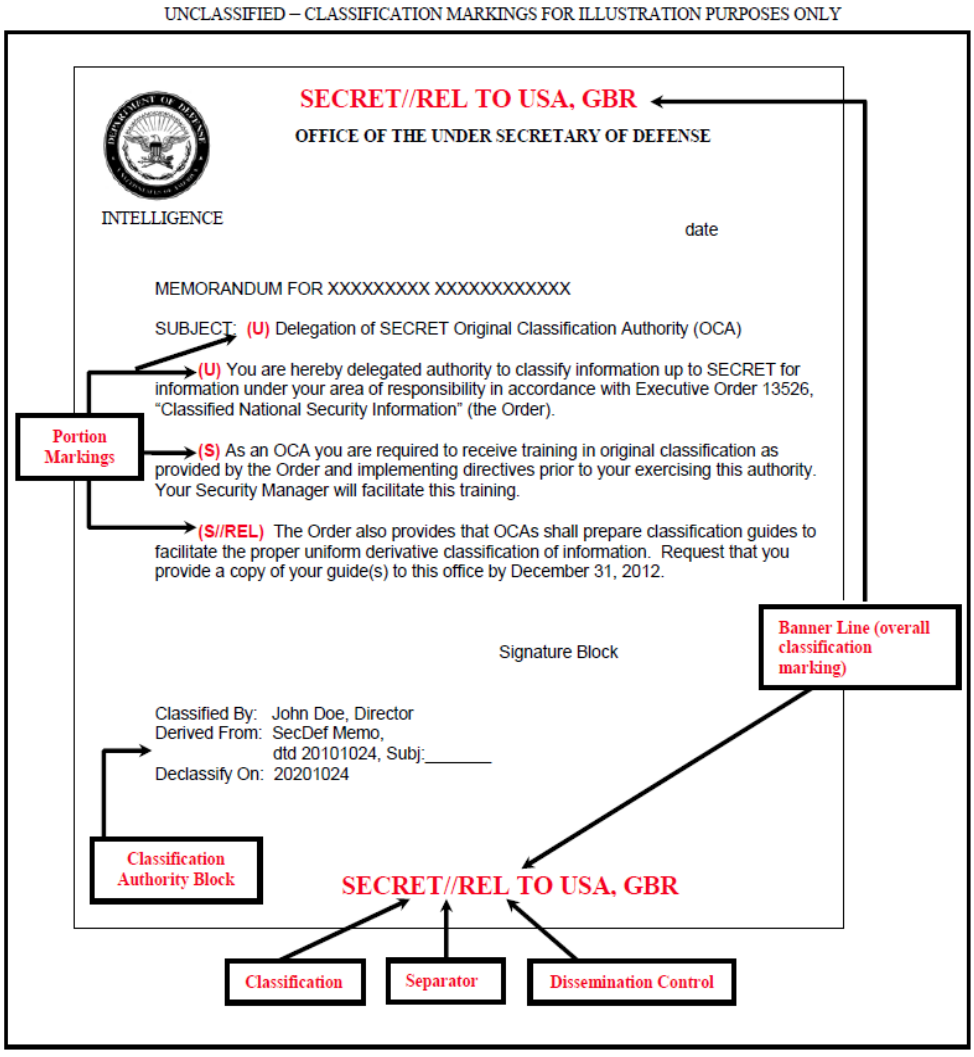
2. Derivative classifiers must include a Derived From Line and cite the source document or classification guide used for the classification determination. The originating component or agency, office of origin, type of document (e.g., memorandum, SCG, or message), subject, and date will be included as available. Information from the derived from line on source documents will not be included; instead, cite the document where information was obtained or extracted. When more than one classification guide, source document, or combinations of these are used, the derived from line will show "Multiple Sources" and the list of sources will be included. If the document has a bibliography or reference list, it may be used as the list of sources. If so, annotate it accordingly to distinguish the sources of classification from other references.

(c) Downgrade To Line. If applicable, identify the lower level of classification at which the document should be safeguarded and date or event upon which the downgrading should take place. Downgrading instructions are used in addition to, not as a substitute for, declassification instructions.

(d) Declassify On Line. Specify the date or event for declassification, exemption category with date or event for declassification, or other declassification instruction corresponding to the longest period of classification among the source or security classification guidance issued by the OCA. Declassification and downgrading instructions, which may be added to the classification authority block when applicable, will be carried forward by the derivative classifier from the source other classification guidance issued by the OCA. The standard format YYYYMMDD will be used when specifying dates in the classification authority block.

(5) Figure 1 provides an example of a properly marked derivatively classified document.

Figure 1. Example of Derivatively Classified Document



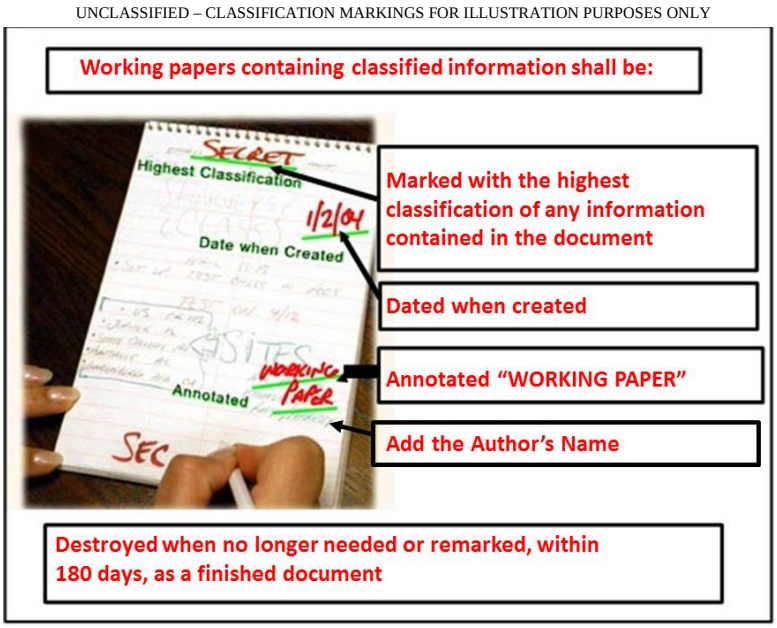
5.3. WORKING PAPERS.

a. Working papers are temporary documents or other materials accumulated or created in the preparation of finished documents and material. Working papers will be marked in the same

manner as a finished document at the same classification level when released by the originator outside the originating activity; retained more than 180 days from date of origin; or filed permanently.

b. E-mail, blogs, wiki entries, bulletin board postings, and other electronic messages transmitted within or external to the originating activity will be marked as finished documents, not as working papers. Figure 2 provides an example of properly marked working papers.

Figure 2. Marking Working Papers



5.4. TRANSMITTAL DOCUMENTS. Transmittal documents often accompany reports and inform readers of a report's context. Transmittal documents include information not found in the report. For example, a transmittal document might contain information about a project and/or due dates. Transmittal documents may be classified or unclassified depending upon content.

a. Transmittal Documents Not Containing Classified Information. Mark Transmittal documents not containing classified information with a banner line with the highest classification level of information contained therein. Also mark the transmittal document with appropriate instructions indicating it is unclassified when separated from its classified enclosure(s) (e.g., "UNCLASSIFIED when separated from classified enclosures" or "UNCLASSIFIED when Attachment 2 is removed").

(1) If any dissemination control markings apply to the transmittal document or any enclosure, include them on the banner line of the transmittal document.

(2) Unclassified transmittal documents do not require portion marking or a classification authority block.

(3) Banner lines are not used on interior pages of unclassified transmittal documents.

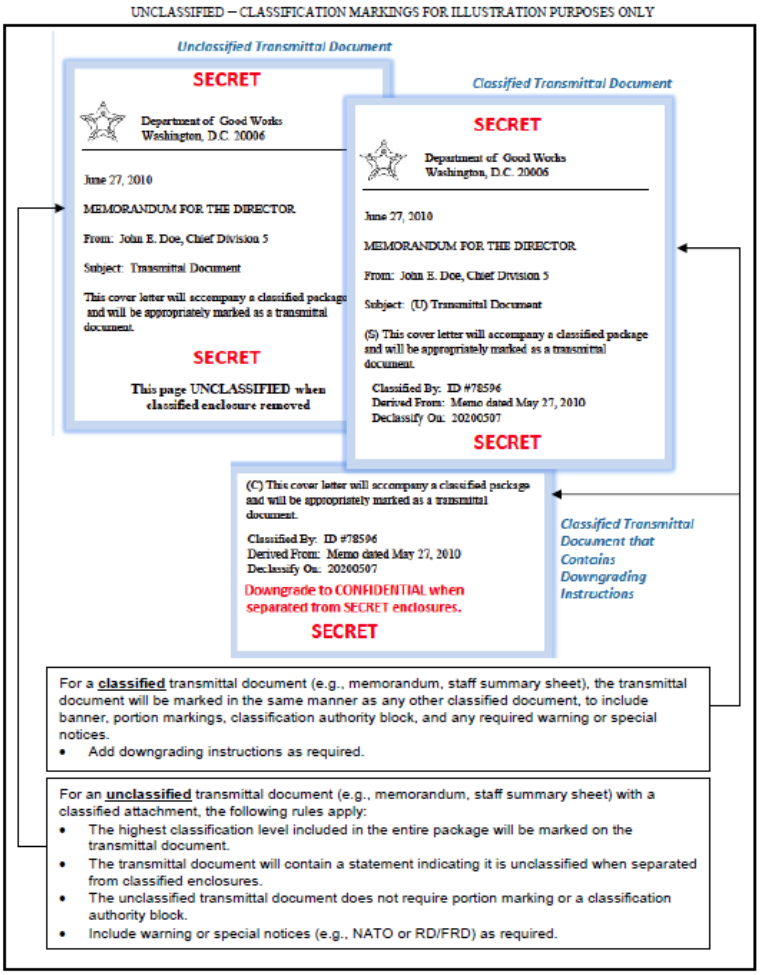
(4) If special notices (e.g., North Atlantic Treaty Organization (NATO), restricted data (RD), formally restricted data (FRD), or export control) apply to the transmittal document or the enclosure(s), include a statement on the face of the transmittal document highlighting inclusion of the information. Unless directed otherwise by applicable policy or regulation, a statement similar to "Document transmitted herewith contains [level of classification] RESTRICTED DATA" or "This document contains NATO [level of classification] information" will suffice.

b. Transmittal Documents Containing Classified Information. Mark with required markings shown in Paragraph 5.2., of this Manual; including banner lines, portion markings, derived from line, classification authority block, and the full text of any applicable special notices.

(1) Mark the banner line of the transmittal sheet with the highest classification level of information contained in the transmittal sheet or its enclosures.

(2) Provide instructions indicating the overall classification level if the level will change when the enclosures are removed (e.g., "Downgrade to CONFIDENTIAL when separated from Secret enclosures"). Figure 3 provides examples of properly marked transmittal documents.

Figure 3. Marking Transmittal Documents



5.5. BRIEFING SLIDES. All slides will be marked when presentations contain classified information or CUI. Ensure to distinguish between classified information and CUI.

a. The first slide will contain the overall classification of the presentation. The remaining slides will be marked either with the overall classification or with the classification of the individual slide. The marking will be large enough to ensure viewers easily recognize the classified information or CUI. The classification authority block will be placed on the first slide.

b. Include the list of sources on the last slide when content of briefing slides is derived from multiple sources.

c. All content portions including bullets, captions, titles, embedded graphs, charts, and figures will be marked to identify classified information and CUI. When marking charts, graphics, or figures, indicate the classification of the individual portion (e.g., bullet, caption, or title) not the overall classification of the chart itself.

c. Mark hidden (backup) slides and speaker's notes to reflect the classification of each portion and the highest classification of each slide or page in the same manner as the remaining slides of the presentation.

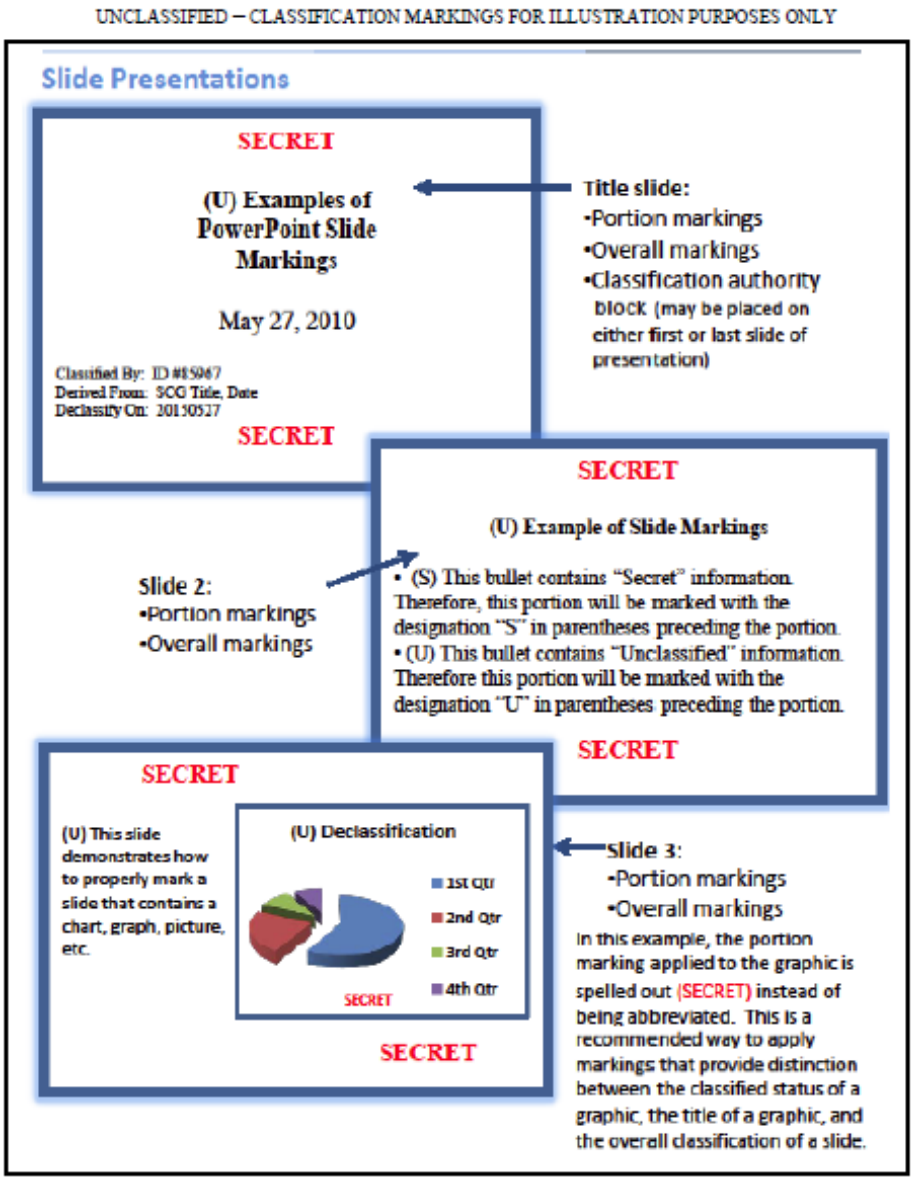
d. On complex slides where portion marking everything would be difficult or would detract from the information on the slide, use the following guidelines:

(1) When all portions contain classified information at the same level, mark only the overall classification of the slide. This indicates all information is classified at the same level.

(2) When a majority of the slide portions are classified, mark the slide with the classification level of the majority of the portions and then portion mark the exceptions. Place a statement on the slide explaining the marking convention. For example, "All portions are classified SECRET unless otherwise marked."

(3) When a majority of the portions are unclassified, portion mark the classified portions and place a statement on the slide explaining the marking convention. For example, "All portions are UNCLASSIFIED unless otherwise marked." Figure 4 illustrates the proper markings for a presentation containing classified material.

Figure 4. Marking Briefing Slides



5.6. MARKING IN THE ELECTRONIC ENVIRONMENT.

a. General. Classified information in the electronic environment is subject to all safeguarding requirements of E.O. 13526, and will be marked as required in DoDM 5200.01, Volume 2, Enclosure 3. All e-mail, blogs, wiki entries, bulletin board postings, and other electronic media will be marked as finished documents due to the originator's inability to control retention and redistribution once transmitted.

b. Electronic Mail (E-mail).

(1) E-mail transmitted on or prepared for transmission on classified systems or networks will display the banner line at the top and bottom of the body of each message. A single linear

text string showing the overall classification, to include dissemination and control markings, will be included as the first line of text and at the end of the body of the message after the signature block.

(2) The banner marking for the e-mail will reflect the highest classification contained in the header and body of the message. The highest classification must also be included in the subject line, the text of the e-mail, any classified signature block, attachments (included messages), and any other information conveyed in the body of the e-mail.

(3) Classified e-mail will be portion marked to reflect the highest level of information contained in the portion. Text portions containing a uniform resource locator (URL) or reference (i.e., link) to another document will be portion marked based on the classification of the content of the URL or linked text, not the content to which it points. This is true even when the data accessible via the URL or link reflects a higher classification marking.

(4) The subject line will be portion marked to reflect the classification of the subject line itself, not the overall classification of the e-mail. Subject lines and titles will be portion marked before the subject or title.

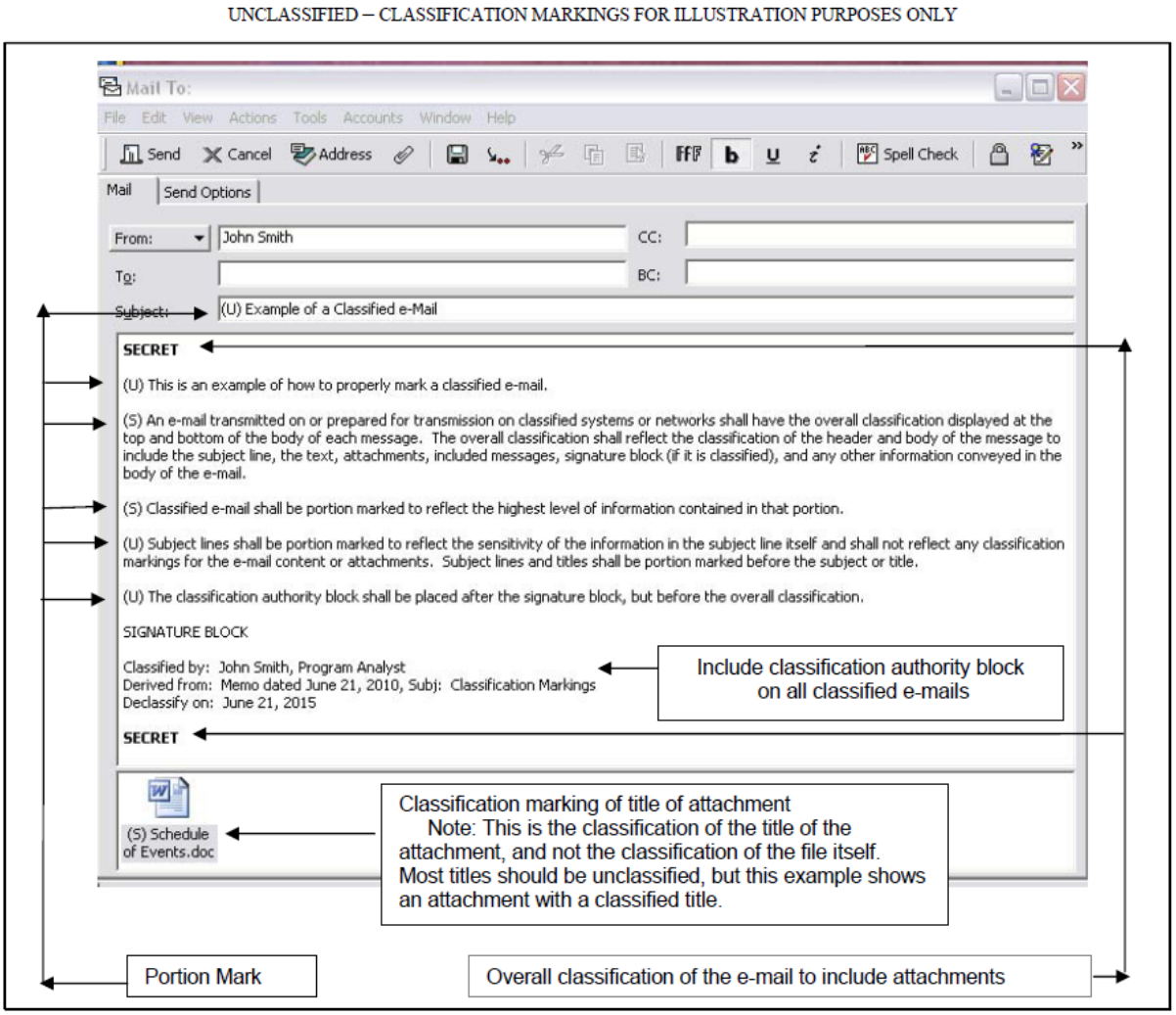
(5) The classification authority block will be placed after the signature block but before the banner line at the bottom of the e-mail. The block may optionally appear as a single linear text string instead of the traditional three line format.

(6) When forwarding or replying to an e-mail, the person transmitting the e-mail will ensure that the markings used reflect the classification markings for all the content present in the resulting message and any attachments. This will include any newly drafted material, material received from previous senders, and any attachments.

(7) For unclassified e-mails or other messages transmitted over a classified system, the designation “UNCLASSIFIED” will be conspicuously placed within the banner line. All applicable dissemination controls (“FOUO” (for official use only), “PROPIN” (proprietary information), etc.) will be included.

(8) E-mails used as transmittal documents will be marked in accordance with Paragraph 5.4. Place the instruction indicating the e-mail’s overall classification level when separated from its enclosures just above the banner line at the bottom of the message. Figure 5 illustrates the proper markings for an e-mail.

Figure 5. Marking E-mails



c. Web Pages.

(1) Mark web pages based on content regardless of the classification of the pages to which they link. Information to which the web page links will also be marked based on its content.

(2) The banner markings for a Web page will reflect the overall classification markings and any dissemination control or handling markings for the information on that page. Linear text appearing on both the top and bottom of the page is acceptable.

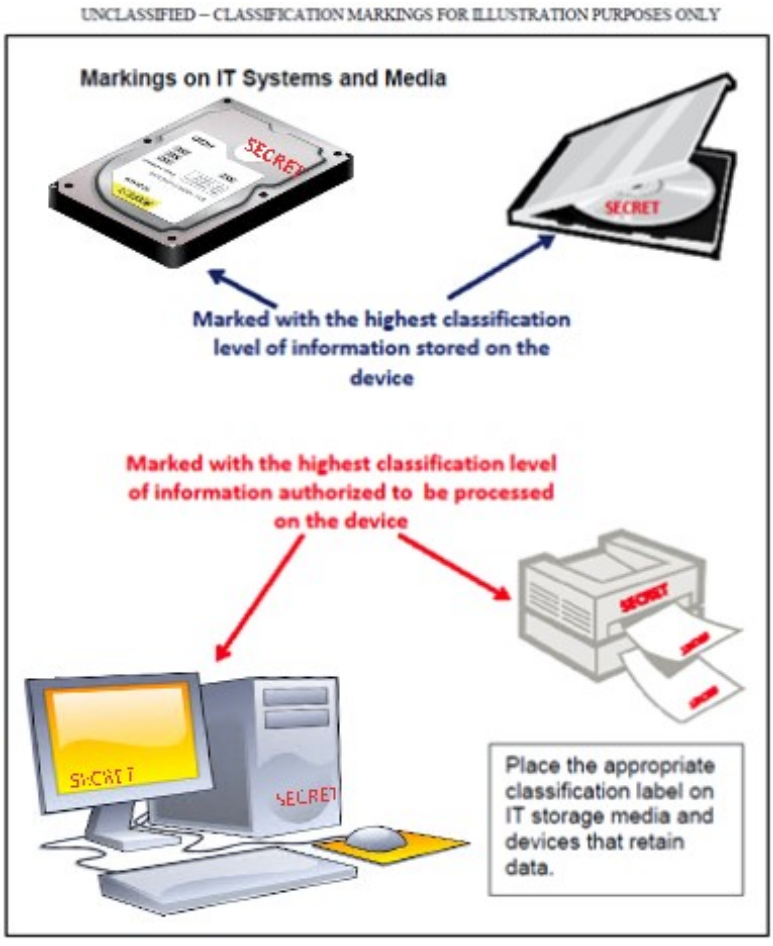
(3) If any graphical representation (e.g., picture, chart, diagram or other graphic) is utilized, a text equivalent of the overall classification marking string will be included in the hypertext statement and page metadata. This will enable users without graphic display to be aware of the classification level of the page and allows for the use of text translators.

(4) Classified information located on Web pages will be portion marked. Each portion will be marked to reflect the highest level of information contained in the portion. A portion containing a URL or reference to another document will be portion marked based on the classification of the content of the URL itself, even if the content to which it points requires a higher classification marking.

d. Marking Media.

(1) Conspicuously mark removable storage media used with computers, information technology (IT) systems, and other electronic devices (see Figure 6). Examples of such media include, but are not limited to, compact discs (CD), digital versatile discs (DVD), removable hard disks, flash or thumb drives, magnetic tape reels, disk packs, floppy disks and diskettes, disk cartridges, optical discs, paper tape, magnetic cards, memory chips, and tape and micro-cassettes.

Figure 6. Marking Computer Equipment and Media



(2) Internal media (for example, a hard drive mounted inside a desktop computer) must include security markings in a form suitable for the media. All such devices bearing classified information must be conspicuously marked with the highest level of classification of information stored on the device and any dissemination control notices that apply to the information.

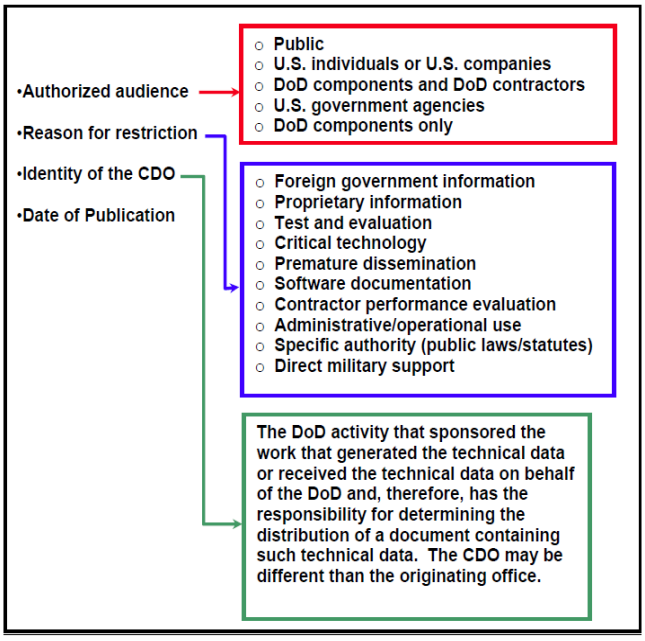
(3) Use Standard Forms (SF) 706, "Top Secret (Label)," SF 707, "Secret (Label)," SF 708, "Confidential (Label)," or SF 710, "Unclassified (Label)," as appropriate, to identify the highest level of classified information stored on IT systems and removable IT storage media. Where size or technology preclude affixing labels to the removable device itself (e.g., memory chips), the label may be affixed to the sleeve or container in which the device is stored.

e. Other Types of Materials. Blueprints, engineering drawings, charts, maps, and similar items not embedded in a classified document will be marked with the appropriate overall classification and dissemination control markings. The classification markings will be unabbreviated and conspicuously applied to the top and bottom in such a manner as to ensure reproduction on any copies. The legend or title will also be portion marked to show classification of the legend or title. If blueprints, maps, and other items are large enough that they are likely to be rolled or folded, the classification markings will be placed to be visible when the item is rolled or folded.

5.7. DISTRIBUTION STATEMENTS.

a. Distribution statements are used on classified and unclassified scientific and technical documents to identify the document's availability for distribution, release, and disclosure without additional approvals and authorizations from the controlling DoD office (CDO). Each statement provides four pieces of information, as illustrated in Figure 7, to facilitate secondary distribution and release.

Figure 7. Information Provided by Distribution Statements



b. Persons generating or responsible for technical documents will determine each document's secondary distribution availability and mark it in accordance with DoDD 5230.24 before primary distribution. Authorized distribution statements are shown in Table 1. The

distribution statement will be placed conspicuously on the cover page or first page of the document.

Table 1. Authorized Distribution Statements

DISTRIBUTION STATEMENT A.	Approved for public release; distribution is unlimited.
DISTRIBUTION STATEMENT B.	Distribution authorized to U.S. Government Agencies only (fill in reason) (date of determination). Other request for this document will be referred to (insert controlling DoD office).
DISTRIBUTION STATEMENT C.	Distribution authorized to U.S. Government Agencies and their contractors (fill in reason) (date of determination). Other requests for this document will be referred to (insert controlling DoD office).
DISTRIBUTION STATEMENT D.	Distribution authorized to the DoD and U.S. DoD contractors only (fill in reason) (date of determination). Other requests will be referred to (insert controlling DoD office).
DISTRIBUTION STATEMENT E.	Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests will be referred to (insert controlling DoD office).
DISTRIBUTION STATEMENT F.	Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD authority.
DISTRIBUTION STATEMENT X.	Distribution authorized to U.S. Government Agencies and private individuals or enterprises eligible to obtain export controlled technical data in accordance with DoDD 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure" (date of determination). Controlling DoD office is (insert).

(1) Documents recommended for public release (Distribution A) must first be reviewed in accordance with DoDD 5230.09, "Clearance of DoD Information for Public Release" prior to any release.

(2) All security classification and declassification guides incorporating technical data will be marked with the appropriate distribution statement.

(3) All documents containing export-controlled technical data will be marked with the export-control statement specified by DoDD 5230.24.

c. DCMA personnel must review the DD Forms 1423, "Contract Data Requirements List" (CDRL) associated with the contracts they are supporting for guidance concerning application of the proper distribution statement to technical documents originated in support of contracts.

5.8. NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN).

a. The dissemination marking NOFORN is an intelligence control marking used to identify intelligence information an originator has determined meets the criteria of Intelligence Community Directive (ICD) 710, "Classification and Control Markings System" and may not be

provided in any form to foreign governments (including coalition partners), international organizations, foreign nationals, or immigrant aliens without the originator's approval.

b. Within DoD, NOFORN is authorized for use **only** on intelligence-related information and products under the purview of the Director of National Intelligence (DNI) with two information exceptions, which are to be marked NOFORN. The exceptions are:

(1) Naval nuclear propulsion information (NNPI). NNPI processed and handled within DCMA is predominately CUI. This form of unclassified information has specific handling, storing, and dissemination protections.

(2) National Disclosure Policy-1 (NDP-1), "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations." Other than these exceptions, there is no authorized DoD use for the NOFORN caveat on non-intelligence information or products.

5.9. SENSITIVE COMPARTMENTED INFORMATION (SCI) CONTROL SYSTEM MARKINGS.

a. SCI is classified national intelligence information concerning, or derived from, intelligence sources, methods or analytical processes that require handling within formal access control systems established by the DNI.

b. The published SCI control systems are:

- Human Intelligence Control System (HCS)
- KLONDIKE (KDK)
- Communications Intelligence (COMINT), also known as Special Intelligence (SI)
- TALENT KEYHOLE (TK)

c. Any DCMA employee finding material carrying the markings identified in Paragraph 5.9. of this Manual outside an approved SCIF will immediately notify the servicing RIS or DCMAS PSO (as applicable).

5.10. SPECIAL ACCESS PROGRAM (SAP) INFORMATION.

a. General. A program activity having enhanced security measures, imposing safeguarding and access requirements exceeding those normally required for information at the same level. Information requiring protection within a SAP is identified by an SCG. The level of controls applied to SAP information and materials is based on the criticality of the program and the assessed hostile intelligence threat. The SAP may be an acquisition program, an intelligence program, or an operations and support program.

b. Handle Via Special Access Channels Only (HVSACO). The purpose of HVSACO is to preclude the disclosure of critical program information and general program related information outside established acknowledged and unacknowledged SAP channels.

(1) Dissemination of information warranting HVSACO protection will be limited to persons briefed into the SAP and must be retained within SAP approved channels. The term SAP channels denote secure, approved SAP communications systems, SAP facilities (SAPF), or DCMAS PSO-approved SAP storage areas.

(2) SAP information or materials marked Unclassified/HVSACO will not be stored or processed at DCMA facilities not approved or accredited by cognizant Office of the Secretary of Defense (OSD), service component Special Access Program Central Office (SAPCO) or DCMA Special Program Directorate SAP authorities. HVSACO information will not be loaded or transmitted through DCMA computer systems not approved by the DCMAS PSO.

(3) All SAP-related work and information are handled and controlled by the DCMAS. Questions regarding access, control, handling, processing, transmission, or disposition of SAP information will be directed to the DCMAS PSO or other responsible DCMAS authority.

5.11. COVER SHEETS AND STANDARD FORM LABELS.

a. All files, folders, and similar groups of documents containing classified information will have clear classification markings on the outside of the folder or holder indicating the highest classification level of information stored therein. The appropriate classified information cover sheet attached to the front and back of the folder or holder satisfies the requirement. Approved classified information cover sheets are:

- SF 703 – Top Secret Cover Sheet
- SF 704 – Secret Cover Sheet
- SF 705 – Confidential Cover Sheet

b. Use the approved SF classification labels (SF 706, SF 707, and SF 708 (addressed in Paragraph 5.6. of this Manual)) to identify the highest level of classified information stored on IT systems and removable electronic storage media. These labels may be used on other items to clearly identify the classification level of the information contained in or on that item, when appropriate. All destruction devices used for the destruction of classified information will identify the highest level of classified information approved to be destroyed on the device by affixing the appropriate SF label.

c. In environments processing or storing classified information, the SF 710 will be used to identify media or equipment used to processing or storing unclassified information. There is no requirement to use the SF 710 in environments where no classified information is processed or stored.

d. SF labels and cover sheets may be requested by contacting the responsible RIS.

SECTION 6: SAFEGUARDING CLASSIFIED INFORMATION

6.1. GENERAL.

a. All DCMA personnel who work with classified information are personally responsible for safeguarding the information and taking all necessary precautions to prevent access by unauthorized persons. This requirement includes safeguarding classified information known, possessed, or controlled by DCMA personnel. All DCMA personnel will comply with pre-publication security review processes outlined in DoDD 5230.09. Classified information will be protected at all times either by storing in properly constructed and approved open storage areas, vaults, General Service Administration (GSA) approved security containers, or by personal observation and direct control of an individual with appropriate access.

5.1.2. Classified information not under the personal control and observation of an authorized person must be safeguarded in accordance with Section 7 of this Manual and DoDM 5200.01, Volume 3.

6.2. DETERMINING THE NEED FOR ACCESS.

a. General Requirements.

(1) No person will have access to classified information unless they meet the following conditions:

(a) The individual will have an adjudicated security clearance issued in accordance with DoDM 5200.02, "Procedures for the DoD Personnel Security Program (PSP)." Each individual with access to the classified information must have a security clearance granted equal to or higher than the classification level of the classified information concerned.

(b) The individual must have a signed SF 312, "Classified Information Nondisclosure Agreement (NDA) on record."

(c) A determination is made by the person with control of the information that the individual's access to the classified information is essential to the accomplishment of a lawful and authorized Government function (i.e., the individual has a mission-related need-to-know).

(2) The individual with authorized possession, knowledge, or control of classified information has the final responsibility for establishing whether a prospective recipient of the classified information is authorized access to the information. Any question regarding an individual's security clearance and completion of an NDA will be referred to the DCMA Security personnel security (PERSEC) team.

b. Access to Sensitive Compartmented Information (SCI).

(1) Information or materials designated SCI require more stringent and formal access restrictions than collateral classified information. The vast majority of work involving SCI

within DCMA is assigned to DCMAS. Access to SCI outside DCMAS will be strictly limited to those individuals who can clearly demonstrate a specific mission-related requirement that cannot be met by currently cleared personnel assigned to DCMAS. When such a requirement exists, the following process will be followed to request SCI access.

(a) The individual requiring SCI access will report the requirement, with justification, to their Component Head or CMO commander.

(b) The Component Head or CMO commander will review the request against the organization's assigned mission to determine if the justification warrants SCI access.

(c) When it is determined mission requirements warrants such access, the responsible Director or Commander will forward a written request (encrypted e-mail is acceptable) for SCI access to the DCMA PERSEC Team for coordination and consideration. At a minimum, the request will include the following information on the individual being recommended:

- Full name and grade
- Social security number
- Organization
- Current security eligibility
- Justification for access to SCI

(d) Upon receipt of a request, the PERSEC Team will forward the request to the DSCI and the Executive Director, DCMAS, for review and consideration. The Executive Director, DCMAS, will review the justification to determine if the mission requirement can be performed by cleared DCMAS personnel. DCMAS representatives will conduct the necessary coordination to develop a recommendation and response to the request.

(e) The DSCI and the Executive Director, DCMAS, will jointly render a decision on the request and forward the decision to the DCMA PERSEC Team for action, as appropriate.

c. Access to SAP Information. See DCMA-MAN 4201-07, "Personnel Security," for guidance on access to SAP information.

d. Access to NATO Information. See DCMA-MAN 4201-07 for guidance on to NATO information.

e. Access to FGI. Individuals with authorized access to U.S. Government classified information are authorized access to classified FGI of a comparable level in accordance with DoDM 5200.01, Volume 3, Enclosure 4.

f. Access to Planning, Programming, Budget and Execution (PPBE) Information.

(1) In accordance with DoDD 7045.14, "The Planning, Programming, Budgeting, and Execution (PPBE) Process," and OSD Memorandum, "Request for Contractor Access to Planning, Programming, Budgeting, and Execution (PPBE) Documents and Data," DoD military

and civilian personnel possessing a valid security clearance equal to or higher than the classification level of the PPBE information concerned and with a valid need-to-know may have access to PPBE material.

(2) Contractors will not be granted access to PPBE information or materials without written approval of the responsible disclosure authority(s) identified in DoDD 7045.14, Enclosure 3.

(a) Should a DCMA Component Head determine a contractor requires access to PPBE information or materials, the component head will prepare and submit to the appropriate disclosure authority, through the Executive Director, Finance and Business Operations Directorate, a request for contractor access to PPBE.

(b) All requests prepared and submitted will be in compliance with the requirements outlined in DoDD 7045.14 and OSD Memorandum.

(c) The DCMA component head will ensure all contractual and non-disclosure agreement requirements are met in accordance with DoDD 7045.14, prior to the preparation and submittal of requests.

g. Access to Cryptographic or Communications Security (COMSEC) Information and Materials. DCMA-MAN 3301-09, "Communications Security," provides guidance regarding access to COMSEC information and materials.

6.3. VISIT REQUESTS.

a. DCMA Employee Visit Requests.

(1) DCMA employees conducting visits to organizations other than their assigned duty location (DCMA, contractor facility, or other DoD or U.S. Government organization, etc.) and access to classified information is required as a part of the visit, either the employee or the organizational security representative will contact the organization where the visit will take place to identify any clearance verification requirements established by the host.

(2) When clearance verification criterion is identified, the security representative will validate the DCMA employee's clearance and submit the clearance verification based on the requirements established by the organization to be visited. If assistance is required in completing and submitting the clearance verification, assistance may be obtained from the DCMA Security PERSEC team.

b. Visit Requests for Persons Visiting DCMA Locations.

(1) DCMA activities hosting visitors to their organization will determine if the visit requires access to classified information.

(2) If access to classified information is required, the responsible Commander or Director (or designated representative) will ensure all visitors meet the appropriate access requirements in Paragraph 6.2. of this Manual.

(a) DCMA Visitors. Commanders or Directors of DCMA organizations will appoint a person to validate visitor access to classified information. The DoD Joint Personnel Adjudication System (JPAS) will be used to conduct the validation. Direct questions relating to acquiring access to or the use of JPAS to the DCMA Security PERSEC team.

(b) Other DoD or U.S. Government Visitors. DCMA employees hosting visitors from other DoD or other U.S. Government organizations requiring access to classified information as part of the visit, will obtain the DCMA organizational Security Management Office (SMO) code of the location hosting the visit. The DCMA Security PERSEC team can be contacted if assistance is required in identifying the SMO code. Prior to the visit, the DCMA sponsor will validate all requirements for access to classified information (appropriate security clearance, completed NDA, and need-to-know) by the visitors are satisfied.

(c) Contractors. Contractor visits requiring access to classified information must be in support of active contracts. Contracts containing requirements associated with or supporting classified information must have the requirements and protective measures for the classified information identified in a DD Form 254. If a DD Form 254 exists, JPAS will be used to submit and receive visit authorizations. Contractor visitors will be provided with the DCMA organizational SMO code for the transmission of clearance verification. Should the contractor's security office not use JPAS, a visit authorization letter (VAL) must be provided as outlined in DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)." Prior to the visit, the DCMA sponsor will validate all requirements for access to classified information by the visitors are satisfied.

c. Foreign Visits. DCMA-MAN 4201-19, "Foreign Visits and Assignments," provides guidance and requirements associated with foreign visits and assignments to DCMA organizations and facilities by foreign nationals.

6.4. PROTECTION OF CLASSIFIED INFORMATION WHEN REMOVED FROM APPROVED STORAGE.

a. Personnel removing documents containing classified information from approved storage will ensure the documents are covered with an approved cover sheet. Approved classified information cover sheets are address in Paragraph 5.11., of this Manual. The cover sheet will be affixed to the documents.

b. Items containing classified information will remain under the positive control of persons with authorized access to the information when not in approved storage. Prior to transferring safeguarding responsibility to another person, the holder of the classified information will ensure the requirements in Paragraph 6.2.a. of this Manual are met.

6.5. END-OF-DAY SECURITY CHECKS.

a. Each DCMA organization processing, storing, or generating classified information or with classified information storage capability will conduct end-of-day security checks. Checks will be conducted to ensure classified material is properly secured and stored.

b. The SF 702, "Security Container Check Sheet," will be used to record end-of-day security checks on each security container drawer, vault door, or secure room door equipped with an electromechanical lock. The time and initial of persons conducting checks will be recorded in the "Checked By" column. Checks are required even when the container is not opened during the timeframe associated with the check.

c. Rooms or immediate areas housing security containers with classified information storage capability will be checked at the close of each working day or each time the room or area is accessed. Checks will be annotated on the SF 701, "Activity Security Checklist." Additional security and safety check items may be added in the blank spaces on the SF 701.

d. All equipment associated with classified information processing or storage (security containers, secure room or vault doors, secure terminal equipment (STE), KIVs, secure FAX, etc.) will be listed on the SF 701 for inclusion in the end-of-day checks.

6.6. EMERGENCY PLANS FOR THE PROTECTION OF CLASSIFIED INFORMATION.

a. To minimize risk of compromise or loss of classified information, DCMA organizations with classified information storage or processing capability will establish site specific plans for the protection of information in the event of fire, natural disaster, civil disturbance, terrorist activity, or enemy action.

b. The level of detail in emergency plans and amount of testing and rehearsal required to ensure the plans are executable in times of emergency will be based on a risk assessment. As a minimum, plans will detail returning classified information to security containers, closing, and security the security container, if at all possible during emergencies.

c. Site-specific emergency plans may be documented in an overarching organizational security plan or developed separately. If developed separately, emergency plans will be referenced in the organizational security plan.

d. A copy of the site-specific emergency plan for the protection of classified information will be posted in the immediate vicinity of the security container, immediately inside secure rooms or vaults.

e. Emergency plans will be exercised at least annually with exercise results documented in a memorandum for record (MFR) and the MFR will be maintained for at least one year, until superseded by a new MFR.

6.7. SECURE COMMUNICATIONS.

a. Only secure communications circuits approved for the transmission of classified information at the specific level of classification for information to be discussed will be used for discussion involving classified information. For example, information classified at the secret level may only be transmitted over circuits approved for the transmission of secret or higher information.

b. This includes communication by telephone, FAX, e-mail, and other forms of electronic communications. Section 8 of this Manual provides basic secure transmission operational procedures. For a more comprehensive explanation of DCMA secure communications requirements and capabilities, refer to the DCMA-MAN 3301-09.

6.8. EQUIPMENT USED FOR PROCESSING CLASSIFIED INFORMATION.

a. Classified Information Processing (Non-SCI or SAP).

(1) Only information systems (computers, networks, peripherals, etc.) specifically approved by the DCMA designated approving authority (DAA) for processing classified information will be used to process classified information. All requests for the capability to process classified information via a computer or network will be coordinated with and approved by DCMA Information Assurance Division (DCMA-ITK) and the ISPM.

(2) Computers approved for processing classified information will not be connected to any unclassified network (this includes the DCMA's wide area network (WAN), copiers, printers, etc.). No modification to the information systems (IS) physical configuration, to include peripheral attachments (universal serial bus (USB) connectable printers or other devices), are authorized.

(3) Unless approved by the DCMA DAA, the use of wireless or Bluetooth enabled equipment (cellular phones, Blackberry devices, headphones, etc.), are not authorized in areas where classified information processing is conducted.

b. SAP Information Processing.

(1) All systems and networks processing SAP information will be protected according to ICD 705, "SCIFs"/Intelligence Community Technical Specifications (ICS) for Construction and Management of SCIFs 705, and by the continuous employment of appropriate administrative, environmental, and technical security measures. These measures will encompass individual accountability, access control, enforcement of least privilege, auditing, labeling, and data integrity.

(2) SAP information will only be processed on ICD/ICS 705 accredited system approved by the PSO in facilities accredited to the level of information to be processed. Questions concerning requirements of the ICD/ICS 705 will be referred to the DCMAS.

c. SCI Processing.

(1) SCI will only be processed on approved computers connected to the Joint Worldwide Intelligence Communications System (JWICS). Refer to DCMA-INST 1091 concerning SAP information processing.

(2) Computers and network nodes will only be secured in SCIFs built in accordance with ICD/ICS 705.

d. Computing Equipment, Media, and Electronic Devices Safeguards.

(1) Computers used for processing and storing classified information will be provided sufficient protection in accordance with DoDM 5200.01, Volume 3.

(a) Open storage areas, secure rooms, vaults, and Information Processing Systems (IPS) security containers storing computers and other electronic devices used to process, store, or produce data containing classified information must be approved in writing by the ISPM.

(b) Approval for open storage of classified information will be considered following an initial survey of the respective areas. The survey will be conducted by the DCMA Security INFOSEC team using criteria based upon the DoDM 5200.01, Volume 3 and this Manual.

(2) Protect and mark information system equipment, removable hard disk drives, and other media at the highest level of security classification processed or stored on the system. Use the corresponding SF 700 series label for marking. Should the application of SF 700 series labels not be possible, mark the equipment or devices by other permanent means.

(3) Removable media (CDs, removable hard disc drives, etc.) approved by the DAA for processing and storage of classified information will be marked and stored per the highest level of classification of information stored on the media.

(4) Equipment used solely to process unclassified information and used in areas where classified information is processed or stored, must be marked with the SF 710.

(5) All other equipment used to process classified information such as typewriters, dot-matrix printers, video tapes, or other items will be protected and marked appropriately, at the level of classification of the information processed thereon.

(6) Equipment capable of processing or storing classified information or located in areas where classified information is processed or stored in the electronic environment will not be removed from the area unless approved by DCMA-ITK or ISPM.

(7) Used toner cartridges may be treated, handled, stored, and disposed of as unclassified material when removed from equipment provided least five pages of unclassified text was processed through the associated equipment in the last print cycle.

6.9. AREAS APPROVED FOR CLASSIFIED DISCUSSIONS.

a. Areas approved for discussions involving classified information must have physical security safeguards in place to restrict access to authorized personnel. In locations were the immediate exterior of areas used for discussions or presentations involving classified information are conducted are uncontrolled, a DCMA employee with access equal to or greater than the classification level of the information to be discussed will be positioned to maintain immediate visual control of the exterior area. This is to prevent inadvertent disclosure of classified information.

b. All doors, windows, and other openings must be closed during presentations and discussions involving classified information.

c. Areas used to conduct the meetings involving classified information must provide acoustical safeguards to prevent advertent disclosure of information. A sound transmission class (STC) of at least 45 must be achieved before areas are approved for discussions involving classified information.

d. Electronic acoustic safeguards, such as "white noise" devices must be installed and in use before beginning any discussions involving classified information in areas under the control of DCMA. The DCMA Security INFOSEC team can assist in acquiring acoustical countermeasure devices.

e. Visual obstructions must be in place and in use to prevent inadvertent disclosure of information to persons on the exterior or in the immediate entryway of areas where classified information is openly visible.

f. When persons without approved access must enter areas where classified information is in use, the persons' entry must be delayed until the information can be either returned to secure storage, covered, or otherwise protected to prevent inadvertent disclosure visually or acoustically. Persons entering areas where classified information or CUI is present, without appropriate access will be escorted at all times by a DCMA government employee. The DCMA employee will be cleared to a level equal to or greater than the information in use in the area.

6.10. CLASSIFIED INFORMATION REPRODUCTION.

a. Reproduction of classified information (paper copies, electronic files, etc.) is strictly limited to the minimum number of copies necessary for mission accomplishment. All limitations and restrictions concerning reproduction by the responsible OCA will be observed.

b. Reproduction of products containing classified information is allowed only under the following conditions:

(1) Reproduce only the minimum amount required for mission accomplishment.

(2) Products containing classified information will only be reproduced on devices with written approval by the ISPM or DCMAS PSO (as applicable) by memorandum.

(a) Approval memorandums are for specified, designated devices. The approval memorandums must be posted in the immediate and direct vicinity of the devices. The memorandums will have the following information related to the subject device:

- Manufacturer name
- Model
- Type of device
- Level of classified information approved for production
- The exact location of the device (address, building, room or area, etc.)
- Date of approval

(b) A copy of all approval memorandums must be kept on file in the respective DCMA Security INFOSEC or PSO office.

(c) When the associated device receives maintenance or other service by persons without appropriate access for the classified information associated with the device (reproduced, processed, or otherwise stored on the machine), a DCMA government employee with appropriate access equal to or greater than the information on the associated device must be in a position to closely monitor the person providing the maintenance or service at all times.

(3) Persons reproducing products containing classified information will be knowledgeable of the procedures for classified reproduction, the risks involved with the specific reproduction equipment, and will ensure appropriate countermeasures are in place and in use.

(4) Any reproduction limitations established by the responsible OCA or any special controls applicable to special categories of information will be strictly observed.

(5) Reproduced materials will be placed under the same accountability and control requirements as applied to the original material.

(6) Extracts of documents will be marked according to content and may be treated as working papers, as appropriate.

(7) Items to be reproduced will be clearly marked to reflect the applicable classification level.

(8) Copies of items containing classified information will be reviewed after the reproduction process to ensure required markings are readily apparent and applied.

(9) Waste products generated during reproduction will be protected and destroyed consistent with classification requirements.

c. No equipment used to reproduce classified information will be released from DCMA's control without the consent of the ISPM or DCMAS PSO (for DCMAS organizations).

6.11. CLASSIFIED MEETINGS AND CONFERENCES.

a. Meetings, conferences, seminars, exhibits, symposiums, conventions, training courses, and other such venues present unique vulnerabilities and increase the risk for unauthorized disclosure of classified information.

b. DCMA personnel hosting in such forums will establish specific protective measures to safeguard classified information. The respective RIS will be contacted to ensure appropriate safeguards and planning documents are established. For SAP information, refer to DCMA-INST 1091 and contact the DCMAS PSO.

c. Prior to the start of large audience events (at least 45 days or sooner if possible), where classified information will be disclosed, the DCMA responsible management official will review the purpose of the forum to ensure:

(1) The forum will serve a specific U.S. Government purpose.

(2) The use of other appropriate channels for the dissemination of classified information are insufficient.

(3) The forum location will be under the security control of a U.S. Government agency or a U.S. Government contractor with an appropriate facility security clearance.

(4) The site or facility meets the applicable physical security standards, including proper acoustical safeguards, approved storage, and approved destruction capabilities.

(5) Equipment (computers, projection devices, copiers, printers, etc.) used at the site to process or reproduce classified information meets or exceeds DAA requirements. All DCMA equipment used to process, present, or store classified information must be approved by DAA.

(6) Adequate security procedures are developed and implemented to minimize risk of inadvertent disclosure of classified information.

(7) Discussion sessions or presentations where classified information is involved will be segregated from unclassified sessions whenever possible.

(8) Access to classified forums or specific sessions, where classified information will be discussed or disseminated, will be limited to persons who possess an appropriate security clearance and need-to-know as validated by an authorized visit certification.

6.12. SENSITIVE COMPARTMENTED INFORMATION (SCI).

a. SCI will be controlled and protected in accordance with ICD 705, “Sensitive Compartmented Information Facilities,” Intelligence Community Technical Specifications (ICS) for Construction and Management of Sensitive Compartmented Information Facilities 705, Version 1.0; ICD 503, “Intelligence Community Information Technology Systems Security:

Risk Management, Certification and Accreditation"; ICD 700, "Protection of National Intelligence"; ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information"; ICD 710, "Classification and Control Markings System"; DoDI 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information." Classified information not governed by the guidance in this paragraph is considered collateral classified information.

b. Security classification and declassification policies of this Manual apply to SCI in the same manner as collateral classified information.

c. SCI will not be received, stored, or processed within non-DCMAS organizations without prior approval of the SSO, DCMAS Security, and/or the ISPM.

6.13. SAFEGUARDING FGI.

a. NATO Information.

(1) NATO classified information will be controlled and safeguarded according to United States Security Authority for NATO Affairs Instruction 1-07, "Implementation of NATO Security Requirements."

(2) Allowing access to NATO classified information will be consistent with Paragraph 6.2. of this Manual.

(3) Receipt of a NATO briefing will be verified prior to granting access to NATO classified information. See DCMA-MAN 4201-07 for guidance on obtaining NATO briefings.

b. Other FGI. Personnel handling, processing, or storing FGI will comply with the requirements contained in DoDM 5200.01, Volume 3.

6.14. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM). DoD uses the marking alternative or compensatory control measures (ACCM) for classified information requiring special security measures. These measures are intended to safeguard classified information related to intelligence, operations, and support information when normal measures are insufficient to achieve strict need-to-know controls and where SAP controls are not required. Additional guidance on safeguarding ACCM information can be found in DoDM 5200.01, Volume 3.

6.15. CAMERAS AND PERSONAL ELECTRONIC DEVICES (PED) IN AREAS APPROVED FOR CLASSIFIED INFORMATION PROCESSING OR STORAGE.

a. Cameras, personal laptop computers, and all other personally-owned or Government-owned personal electronic devices (PED), to include any wireless device (cellular telephones, portable music players such as iPods and MP3 players, pagers, audio and video players/recorders, digital picture frames, electronic tablets or books, and Bluetooth-enabled

equipment), or electronic fitness devices are prohibited from all DCMA spaces authorized to process, discuss, store, transmit, view, or otherwise associated with classified information.

b. Personally-owned thumb drives and optical storage media such as CDs and DVDs are prohibited from DCMA facilities or spaces used for classified information processing or storage.

c. The unauthorized possession or use of a PED may result in its confiscation by DCMA security officials for the purpose of conducting a forensic or physical examination. These devices may be permanently retained, destroyed, or the data contained therein deleted and the devices may not be returned to the owner.

d. There is no expectation of privacy or confidentiality in the content and metadata resident on any device brought into DCMA facilities where classified information is processed or stored.

e. Government-issued electronic devices may only be authorized for introduction into classified information processing or storage areas when approved by the ISPM or DCMAS PSO for areas under DCMAS control.

f. DCMA employees visiting or working in facilities or areas under the direct control or ownership or other government entities, contractors, or private industry will adhere to the controls and safeguards as enacted by these authorities. At no time will DCMA employees attempt to circumvent established protective measures or use their position in an advantage to circumvent established protective measures.

g. Intentional disregard for established protective measures by DCMA employees may result in disciplinary or potential criminal repercussions.

SECTION 7: STORAGE AND DESTRUCTION

7.1. GENERAL STORAGE REQUIREMENTS.

a. Classified information will be secured under conditions adequate to deter and detect access by unauthorized persons. Items such as weapons of any sort, funds, jewels, precious metals, drugs, or other items considered of value and not directly associated with classified information will not be stored in security containers, vaults, or secure rooms designated for classified information storage.

b. An SF 702 will be located on each security container locking drawer, vault or secure room door designated for storing classified information and equipped with an electromechanical lock. The SF 702 is used to record the date, time, and initials of the person performing each opening, closure, and security checks.

c. All vaults, secure rooms, or open storage areas used to store or process collateral (non-SCI or SAP) classified information will be approved in writing by the ISPM (or appointed representative). Facilities storing SCI or SAP information will comply with the guidance contained in Paragraphs 7.5 and 7.6 of this Manual.

d. Neutralization and repair of a security container, vault or secure room door approved for the storage of classified information will be accomplished only by cleared or continuously escorted personnel certified by GSA. Technicians must be certified to perform work on electromechanical locks installed on security container drawers, secure room or vault doors.

e. DCMA organizations storing or processing top secret information will appoint a top secret control officer (TSCO) responsible for the control and destruction of all top secret materials within the organization.

7.2. STORAGE OF INFORMATION BY LEVEL OF CLASSIFICATION.

a. Classified information not under the personal control and observation of an authorized person will be stored in a locked security container, vault, or secure room meeting specific standards.

(1) Top Secret. Top secret information will be stored in compliance with DoDM 5200.01, Volume 3, and Enclosure 3.

(2) Secret. Secret information will be stored in compliance with DoDM 5200.01, Volume 3, and Enclosure 3.

(3) Confidential. Confidential information will be stored in compliance with DoDM 5200.01, Volume 3, and Enclosure 3.

7.3. SECURITY CONTAINERS.

a. Only GSA approved, class 5 or class 6 security containers will be used for the storage of classified information. DCMA organizations with security containers not of these class groups will notify the DCMA Security INFOSEC team, who will program to replace the containers.

b. Security containers used for storage of classified information will be equipped with an electromechanical lock conforming to Federal Specification FF-L-2740B, "Locks, Combination, Electromechanical," (as amended). Locks requiring batteries for operation will not be installed on security containers used for the storage of classified information in DCMA.

c. Field safes will not be used for classified information storage during peacetime operations. These security containers are only approved for use in wartime-theater or other special circumstances.

d. To ensure security container construction compliance, only the DCMA Security INFOSEC team or DCMAS (as applicable), will procure security containers for DCMA organizations. All procurements will comply with the requirements of DoDM 5200.01, Volume 3, and Enclosure 3. Black lettering filing cabinet security containers will not be repaired upon malfunction. The container will be neutralized, decommissioned, disposed of through Defense Logistics Agency (DLA), and a replacement container procured.

e. Maintenance or repairs on security containers will not be conducted by persons not trained and certified by GSA and specified lock approved technical training. All inspections, maintenance, neutralization, and repairs of security containers will conform to Federal Standard (FED-STD) 809C, "Inspection, Maintenance, Neutralization and Repair of GSA Approved Containers and Vault Doors." Unapproved painting, maintenance, or repairs of security containers or locks installed on security containers can invalidate GSA approval for the security container.

f. Regional Command offices, Primary and Streamlined CMOs must maintain classified information storage capability. If a decision is made at the CMO level or below to no longer have classified information storage capability, the responsible Commander or Director will submit a memorandum detailing the decision to the agency ISPM, through the responsible Regional Commander or Executive Director who must approve the decision. The memorandum will show reason for the decision and an executable plan is in place to protect any classified information subsequently received at the location. The originating organization and the ISPM will maintain a permanent record copy of the decision memorandum.

g. Security containers used for storing classified information contained in documents and small items (defined as filing cabinets) will conform to Federal Specification AA-F-358J, "Filing Cabinet, Legal and Letter Size, Uninsulated, Security," (as amended).

f. Security containers will not be changed in any way and will conform to Standard American Equivalent, American Military Standards, Standard (SAE AMS-STD)-595, "Colors Used in Government Procurement," in either gray, black, or parchment. Care will be taken so as to not impede inspection of security containers by permanently affixing stickers, labels, or any other nonapproved items onto either of the six sides (top, bottom, sides) of security containers.

h. Security containers will not be used as a shelf for items (books, folders, plants, coffee pots, water jugs, etc.).

i. Computing equipment and other electronic devices used to process and store classified information in areas, rooms, or other facilities not approved as open storage areas will be stored in GSA approved Information Processing Systems (IPS), conforming to Federal Specification AA-C-2786, "Cabinet, Security, Information Processing System Storage," (as amended).

(1) All requirements listed in Paragraphs 7.3.a. through 7.3.h. of this Manual, are applicable to classified information storage in GSA approved IPS security containers.

(2) All personnel with access to IPS security containers will have an approved SIPRNet account and SIPRNet Token for access through DCMAIT-K Cybersecurity Division.

(3) Special care will be taken to ensure computing systems approved for processing and storage of classified information are secured properly in associated GSA approved IPS security containers. IPS security containers will not be left in the open position unless a person with access to the security container is in close physical proximity of the container.

7.4. VAULTS.

a. Vaults used to store classified information within DCMA will be constructed in compliance with the requirements contained in DoDM 5200.01, Volume 3, Enclosure 3 and FED-STD 832, "Federal Standard: Construction Methods and Materials for Vaults."

b. Maintenance or repairs on GSA approved vault doors and installed electromechanical locks will not be conducted by persons not trained and certified by GSA and specified lock approved technical training. All inspections, maintenance, neutralization, and repairs of GSA approved vault doors will conform to FED-STD 809C. Unapproved painting, maintenance, or repairs of vault doors, frames, or locks installed on vault doors can invalidate GSA approval for the vault door.

c. Vaults used for classified information storage will:

(1) Be equipped with a class 5-V vault door. The vault door and frame will conform to Federal Specification AA-D-600, "Door, Vault, Security."

(2) Be equipped with an electromechanical lock conforming to Federal Specification FF-L-2740B. Locks on vault doors will not require batteries for operation. No other locking devices will be installed on vault doors.

(3) Conform to FED-STD 595, "Colors," (as amended) in gray. Colors of vault doors and frames will not be changed.

d. The DCMA ISPM or DCMAS PSO (or designated representative) will approve in writing vault construction compliance before vaults are used for classified information storage.

e. DCMA will not use modular vaults for storage of classified information. If a module vault is used to store classified information or materials, the module vault will comply with the requirements of DoDM 5200.01, Volume 3, Enclosure 3 and Paragraphs 7.1., 7.2., and 7.4., of this Manual. The DCMA ISPM or DCMAS PSO will approve in writing modular vault use.

f. The DCMA Security INFOSEC Team will procure new vault doors and frames for DCMA organizations to ensure conformity with requirements. All new procurements will comply with the requirements of DoDM 5200.01, Volume 3, Enclosure 3.

g. All vaults will adhere to acoustical safeguards of achieving at least an STC rating of 45 as specified in Paragraph 6.9.c., of this Manual.

h. All vaults will be reviewed on an annual basis by the DCMA Security IPTL or ISPM. This review will be the annual inspection to ensure vaults conform to requirements to meeting classified information open storage.

7.5. SECURE ROOMS.

a. All secure rooms used to safeguard classified information within DCMA will be constructed in compliance with the requirements contained in DoDM 5200.01, Volume 3, Enclosure 3 and this Manual.

b. The ISPM or DCMAS PSO (as applicable) will provide written approval attesting to compliance for secure room construction before the introduction of classified information into the rooms or areas.

c. Secure rooms are authorized to store or process classified information equal to the approved level of classification storage. Secure rooms (open storage areas) will:

(1) Meet all physical security safeguards cited in DoDM 5200.01, Volume 3, Enclosure 3, and each safeguard subject will be addressed prior to approval by the appropriate authority:

- Ceilings or roofs
- Floors
- Walls
- Windows
- Doors
- Openings in the perimeter of the space
- Heating, ventilation, and air conditioning (HVAC) openings
- Intrusion detection systems (IDS)
- Automated Personnel Access Control System (APACS)
- Acoustical protections

(2) Before construction or major renovation of secure rooms, the owning organization will contact the DCMA Security INFOSEC team to ensure all necessary planning considerations are integrated into the project. All necessary requirements will be identified, blueprints of the proposed space reflecting all details of the open storage area, and equipment listing showing protective hardware to be installed will be provided to the DCMA Security INFOSEC team for review, prior to the start of construction or renovation.

(3) The DCMA Security ISPM will provide initial approval of all construction and renovation planning prior to actual work beginning on the space. At detailed intervals, the DCMA Security IPTL or PM will conduct an onsite review of the space.

(a) Ideally, the reviews will be conducted after the space is roughed in with studwork, masonry, and HVAC ducting in place.

(b) A second onsite review will take place when all drywall is in place, doors are hung, and HVAC is completed.

(c) The final construction review will be conducted after all construction is completed and the IDS, APACS, and locks are installed. Approval for open storage of classified information will be granted when all requirements identified in DoDM 5200.01, Volume 3, Enclosure 3 and this Manual are met.

(4) Secure rooms used for the open storage of classified information with false ceiling will:

(a) Have IDS installed above the false ceiling spaces. The IDS will be activated on a separate zone from other IDS zones and will not be disabled or deactivated with other IDS is deactivated for daily activities.

(b) Walls, ceilings, and roof areas located above false ceilings in secure rooms will meet the requirements of DoDM 5200.01, Volume 3, Enclosure 3.

(c) For secure area spaces with false ceilings where IDS is not installed above the false ceiling, the space will be checked at least once every 30 day period. The checks of the space above the false ceiling will be recorded on a written record showing the individuals conducting the checks, results of the checks, and the date and time of the checks.

7.6. SPECIAL ACCESS PROGRAM FACILITIES (SAPF). All areas used to store or process SAP materials within DCMA will be constructed in compliance with applicable intelligence community standards.

7.7. SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIF).

a. All areas used to store or process SCI materials within DCMA will be constructed in compliance with applicable intelligence community standards.

b. The Defense Intelligence Agency (DIA) will accredit DCMA operated SCIFs in writing.

7.8. MARKINGS AND LABELS ON SECURITY CONTAINERS, VAULTS, AND SECURE ROOMS.

a. GSA approved security containers and vault doors used to store classified information will contain a permanent, factory affixed, metallic label stating "GSA Approved Security Container." The label will be affixed to the front of the container or vault door and is normally found on the control or top drawer of containers. GSA approved labels have either black lettering or red lettering with a silver in color background.

b. Security containers or vault doors with missing GSA approved labels will not be used to store classified information until inspected and approved by a GSA certified inspector prior to being placed back in to service. Organizations with containers requiring these inspections may contact the DCMA Security INFOSEC team for assistance.

c. Security containers used to store classified information will not be released to activities external to DCMA unless the containers are sanitized in accordance with the Security Container Neutralization (Sanitation) Check Sheet, located on the DCMA Security INFOSEC resource Web page. The DCMA Security INFOSEC team will be contacted to facilitate all security container transfers. Containers processed through DLA for disposal will have the GSA approved label removed before shipment and a placard stating, "NOT FOR CLASSIFIED INFORMATION STORAGE" affixed to exterior of the container's top drawer.

d. There will be no external markings revealing the level of classified information stored within a security container, vault, or secure room. Markings indicating the priority assigned to the container for emergency evacuation and/or destruction will not be affixed on containers, vaults, or secure rooms. This requirement does not preclude placing a mark or symbol (e.g., a bar code) on the container for identification or inventory purposes, or applying decals or stickers the DNI requires for containers and equipment used to store or process intelligence information.

e. Questions regarding security containers will be referred to the responsible RIS or DCMAS security official (as applicable).

7.9. LOCKING DEVICES AND COMBINATION SAFEGUARDS.

a. Locking Devices.

(1) Minimum Requirements. All locks used to secure classified information will conform to Federal Specification FF-L-2740B, "Locks, Combination, Electromechanical" (as amended). Any question regarding a locks conformance to the cited standard will be directed to the supporting RIS or DCMAS security official (as applicable).

(2) Lock Maintenance. Only GSA certified locksmiths will perform maintenance on locks securing classified information. Locksmiths will be continuously escorted while

maintenance is being performed. For assistance in obtaining lock maintenance, contact the supporting RIS or DCMA security official (as applicable).

(3) Lock Replacement. Report nonoperational locks used to secure classified information or not meeting standards found in DoDM 5200.01, Volume 3, to the supporting RIS or responsible DCMAS security official for immediate replacement.

b. Recording and Safeguarding Combinations.

(1) Combinations to locks securing classified information will be safeguarded and limited to individuals possessing validated access in accordance with Paragraph 6.2., of this Manual to the security container, vault, or secure room storing classified information. All persons with knowledge of combinations for security containers, vaults, or secure rooms will be identified on the lock's associated SF 700, "Security Container Information."

(2) Combinations to locks securing classified information will be classified at the same level as the highest classification of information stored.

(3) Combinations to security containers storing classified information will not be retained on one's person, in a wallet or purse, or entered on a calendar, computers not approved for classified information processing or storage, cellular phones, other electronic devices not approved for classified information processing, or other unauthorized locations.

c. Completing the SF 700.

(1) Combinations to locks securing classified information will be recorded on a SF 700. An SF 700 with all applicable information blocks completed will be maintained for each locking device on security containers, vaults, or secure room doors used for storing classified information. Each time a combination is changed, the associated SF 700 will be updated. All personnel with knowledge of the combination will be identified on the SF 700. The SF 700 serves as the associated security container access control authorization listing.

(2) The SF 700 is a multi-part form consisting of an envelope (Part 2), a tear-off tab (Part 2A), and cover sheet (Part 1). The SF 700 records relevant organizational information, container identification information, lock type, date of combination change, and who to contact if the container is found open.

(3) Part 1 of SF 700 is not classified but contains personally identifiable information (PII). Mark Part 1 of the form "Unclassified//PII" and protect the document by sealing it in an opaque envelope (not provided as part of the SF 700), marked "Security Container Information." Store the envelope containing Part I of the SF 700 in the inside front of the security container control drawer (the drawer with the electromechanical lock). For vault or secure room doors, affix the envelope containing Part I of the SF 700 to the door on the immediate interior of the area protected by the lock.

(4) When completed, Part 2 and Part 2A of the SF 700 are marked at the highest level of classification authorized for storage in the security container, vault, or secure room. Both the completed Part 2 and Part 2A of the SF 700 will be provided protection at a level equal to or greater than the classification level of the classified information stored therein. When completed, tear off Part 2A of the SF 700, insert into the envelope (Part 2), and then seal the Part 2. Mark the Part 2 on the top and bottom, front and rear with the appropriate classification level. Add a classification authority block to the front of the Part 2 stating "Derived from: 32 CFR 2001.80(d)(3))," with "declassify upon change of the combination." Mail the Part 2 to the servicing RIS for safeguarding. For DCMAS organizations, follow the guidance issued by the DCMAS PSO.

d. Changing Combinations.

(1) Only DCMA personnel with the direct responsibility, as assigned by the responsible commander/director, with appropriate access in accordance with Paragraph 6.2., of this Manual and listed on the SF 700 will change combinations to security containers, vaults, and secure rooms used for classified information storage. A record of the names of persons having knowledge of the combination will be maintained and available for review. The SF 700 can be used to satisfy this requirement. (**NOTE**: Combination locks installed on security containers, secure rooms, or vault doors will be reset to the standard combination 50-25-50 when no longer used to safeguard classified information. Combination padlocks will be reset to the standard combination 10-20-30 when no longer used to safeguard classified information.)

(2) Combinations will be changed:

(a) When the container, vault, or secure room door is placed in service.

(b) When individuals with knowledge of the combination to the container, vault, or secure room door no longer requires access.

(c) When compromise of the combination is suspected.

(d) When the container, vault, or secure room door is taken out of service or is no longer used to store classified information.

7.10. U.S. CLASSIFIED INFORMATION LOCATED IN FOREIGN COUNTRIES.

a. Guidance concerning access to classified information in countries other than the U.S. is normally addressed in the applicable status of forces agreement (SOFA) or U.S. Department of State memorandum of agreement.

b. Except for classified information authorized for release to a foreign government or international organization in accordance with DoDD 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," U.S. Government owned classified information may be retained and stored in a foreign country only when necessary to satisfy specific U.S. Government requirements.

c. U.S. classified information located in a foreign country under the control of DCMA will be stored in strict compliance with the requirements of DoDM 5200.01, Volume 3, Enclosure 3 and this Manual.

7.11. RETENTION OF CLASSIFIED INFORMATION.

a. Classified information holdings within DCMA organizations will be retained only if required for the effective and efficient operation of the organization or if required by law or regulation.

b. Classified information no longer required will be returned to the information originator or destroyed by approved destruction means.

c. Commanders or Directors will ensure classified information under their control are reviewed at least annually. Classified information no longer required will be disposed of in an approved manner, accordance with Paragraph 7.12., of this Manual.

7.12. DESTRUCTION OF CLASSIFIED INFORMATION.

a. Classified information identified for destruction will continue to be protected until destroyed. Documents and other items containing classified information will be destroyed when:

- The documents are no longer required for operational purposes or required for retention by statute or regulation
- Return of the information to the originator is not required

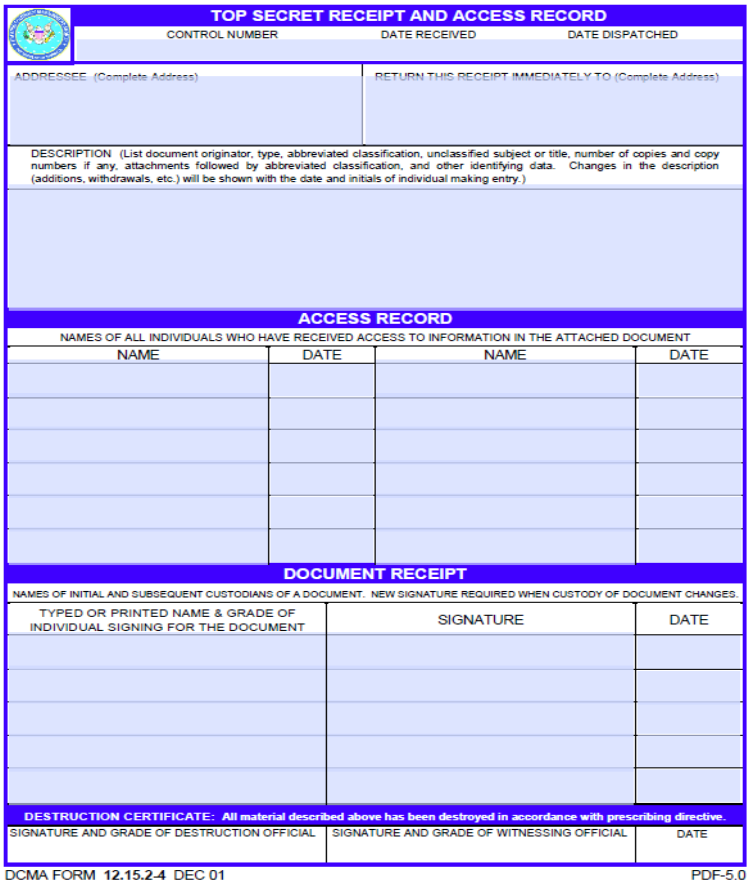
b. Only equipment listed on the National Security Agency (NSA) issuance, "NSA/Central Security Service (CSS) Evaluated Products List (EPL) for High Security Crosscut Paper Shredders," will be used to destroy documents and other materials containing classified information.

c. Dispose of items other than documents containing classified information by use of devices listed on the applicable NSA/CSS EPL. Contact the supporting RIS or ISPM for assistance.

d. Non-DCMAS organizations requiring equipment to support classified information and CUI destruction will notify the supporting RIS of the requirement who will submit the requirement to the ISPM for procurement. Devices will be procured in accordance with Paragraph 7.13., of this Manual.

e. Certificates of Destruction. DCMA organizations storing or processing top secret information will identify and designate a TSCO. The TSCO will ensure a destruction certificate is completed when items containing Top Secret classified information are destroyed. Use DCMA Form 12.15.2-4, "Top Secret Receipt and Access Record" as the official destruction certificate, located on the DCMA INFOSEC resources Web page.

Figure 8. Top Secret Receipt and Access Record



TOP SECRET RECEIPT AND ACCESS RECORD

CONTROL NUMBER	DATE RECEIVED	DATE DISPATCHED

ADDRESSEE (Complete Address)	RETURN THIS RECEIPT IMMEDIATELY TO (Complete Address)

DESCRIPTION (List document originator, type, abbreviated classification, unclassified subject or title, number of copies and copy numbers if any, attachments followed by abbreviated classification, and other identifying data. Changes in the description (additions, withdrawals, etc.) will be shown with the date and initials of individual making entry.)

ACCESS RECORD

NAMES OF ALL INDIVIDUALS WHO HAVE RECEIVED ACCESS TO INFORMATION IN THE ATTACHED DOCUMENT

NAME	DATE	NAME	DATE

DOCUMENT RECEIPT

NAMES OF INITIAL AND SUBSEQUENT CUSTODIANS OF A DOCUMENT. NEW SIGNATURE REQUIRED WHEN CUSTODY OF DOCUMENT CHANGES.

TYPED OR PRINTED NAME & GRADE OF INDIVIDUAL SIGNING FOR THE DOCUMENT	SIGNATURE	DATE

DESTRUCTION CERTIFICATE: All material described above has been destroyed in accordance with prescribing directive.

SIGNATURE AND GRADE OF DESTRUCTION OFFICIAL	SIGNATURE AND GRADE OF WITNESSING OFFICIAL	DATE

DCMA FORM **12.15.2-4** DEC 01 PDF-5.0

(1) Certificates of destruction are not required when destroying collateral secret or confidential classified information.

(2) Destruction of SCI and SAP classified information will conform to the guidance established by the DCMAS PSO and other applicable policies.

7.13. ACQUISITION OF DESTRUCTION DEVICES AND SERVICES

a. Supporting RIS's will assist in identifying the level and size of shredders when needs are identified for classified information for CUI destruction. A request worksheet providing required information for ordering applicable equipment will be completed by the DCMA organization. The DCMA Security INFOSEC Team will procure the necessary equipment with instructions to follow concerning delivery of the unit(s).

b. On site shred service will be requested through the RIS and provided as available. This service saves employee time and equipment costs. The on site shred service is not available at most contractor owned sites where DCMA is co-located.

c. The DCMA Security INFOSEC team supports one time shred events where a site has accumulated large amounts of documents over time and has a need for destruction. Please contact the respective RIS at least 180 days before the service is needed.

SECTION 8: TRANSMISSION AND TRANSPORTATION OF CLASSIFIED INFORMATION

8.1. GENERAL. Physically transmitting or transporting classified information dramatically increases the potential for compromise. Appropriate care, training, oversight, and approval must be implemented to ensure the protection of classified information.

8.2. DISSEMINATION OF CLASSIFIED INFORMATION OUTSIDE THE DEPARTMENT OF DEFENSE. Classified information will only be disseminated outside DoD with the consent of the originating organization or when in compliance with the requirements of DoDM 5200.01, Volume 3, Enclosure 4.

8.3. TRANSMISSION OF CLASSIFIED INFORMATION.

a. Transmission of Top Secret Information. Top secret information will be transmitted in compliance with the requirements established in DoDM 5200.01, Volume 3, Enclosure 4. Questions regarding proper protocols associated with the transmission of top secret information will be directed to the ISPM or the DCMAS PSO (as applicable).

b. Transmission of Secret Information. Secret information will be transmitted in compliance with the requirements established in DoDM 5200.01, Volume 3, Enclosure 4 and this Manual. Questions regarding the transmission of secret information will be directed to the ISPM or the DCMAS PSO (as applicable).

c. Transmission of Confidential Information. Confidential information will be transmitted in compliance with the requirements established in DoDM 5200.01, Volume 3, Enclosure 4 and this Manual. Questions regarding the transmission of confidential information will be directed to the ISPM or the DCMAS PSO (as applicable).

8.4. TRANSMISSION OR TRANSFER OF CLASSIFIED INFORMATION TO FOREIGN GOVERNMENTS.

a. Transmission. Classified information approved for release to a foreign government or international organization will be transmitted in compliance with requirements established in DoDM 5200.01, Volume 3, Enclosure 4 and this Manual..

b. Transfer. All transfers of classified information or material to a foreign government will comply with the requirements established in the appendix to Enclosure 4 of DoDM 5200.01, Volume 3 and this Manual.

c. Command Responsibility. Commanders or Directors responsible for the transmission or transfer of classified information to a foreign government will ensure strict compliance with this Manual. Questions regarding the transfer of classified information to a foreign government will be directed to the responsible program office originating the information or materials. Further assistance can be obtained from the ISPM or the DCMAS PSO (as applicable).

8.5. USE OF SECURE COMMUNICATIONS FOR TRANSMITTING CLASSIFIED INFORMATION.

a. Transmission. The transmission of DoD information will comply with the COMSEC measures and procedures established in DoDI 8523.01, DCMA-MAN 3301-09, and other applicable directives.

b. Computer-to-Computer Transmission.

(1) In addition to meeting the requirements of Paragraph 8.4., of this Manual, computers and other IT systems used for the transmission of collateral classified information will be accredited by the DCMA DAA to operate at a level of classification commensurate with the data being transmitted. All computers and systems used to transmit SAP information will be approved and accredited in accordance with applicable SAP policies and guidelines.

(2) Electronic transmission of classified information over secure computer-to-computer links (e.g., via secure e-mail) is preferable to the physical transfer of hard copy documents. Classified information transmitted in any venue will be properly marked in accordance with DoDM 5200.01, Volume 2, and this Manual.

(3) Computers used for transmitting classified information must not be connected to unclassified networks or peripherals (copiers, printers, etc.). Additionally, computers, network devices, and equipment associated with the transmission of classified information will be secured in an approved security container, secure room or vault, or facility approved for the level of classification transmitted. For example, if collateral classified information (confidential or secret) is transmitted via SIPRNet, the SIPRNet computer terminal, nodes, and other associated equipment will be secured in a secure room or vault meeting the requirements of DoDM 5200.01, Volume 3, Enclosure 3 and this Manual. The secure rooms or vaults will be approved by the ISPM for open storage in accordance with this Manual. For SAP information, the transmission system will be secured in a SAPF or SCIF. The transmission system must be secured in a SCIF if SCI is transmitted.

c. FAX Transmission. Use only approved secure FAX equipment when transmitting classified information. Adhere to the following safeguards when transmitting classified information over secure FAX:

(1) Initiate a telephone call using a secure voice telephone connected to the secure FAX.

(2) The individual transmitting the information will ensure the recipient is approved for access in accordance with Paragraph 6.2., of this Manual and the connection is at the appropriate level of classification for the information to be transmitted.

(3) Cover sheets clearly marked with the highest classification level of the information transmitted will precede the first page and will follow the last page of documents containing classified information. Ensure to include any control markings on the cover sheet s and transmitted document as appropriate.

(4) The cover sheet will include the originator's name, organization, and contact information (telephone number, e-mail, etc.).

(5) An unclassified title and the number of pages must be used.

(6) Add the receiver's name, organization, and phone number.

(7) When the cover sheet contains no classified information, it will also note "Unclassified When Classified Attachment(s) Are Removed."

(8) Documents transmitted by FAX will have all markings required for a finished document and will be controlled and safeguarded accordingly by the recipient.

d. Secure Telephone.

(1) Only secure telephones authorized by the Director, NSA, and approved by the DCMA COMSEC PM, in accordance with DoDM 5200.01, Volume 3, Enclosure 4, and this Manual, may be used for telephonic transmission of classified information. Users must ensure the connection is secured at the appropriate level of classification for the classified information to be discussed.

(2) Acoustical countermeasures in accordance with Paragraph 6.9. of this Manual will be in place before discussions involving classified information at the Secret level or below are conducted.

(3) Remove KOV-14 cards from STE's and store in accordance with DCMA-MAN 3301-09 to ensure proper safeguards when STE's are unattended. Secure telephone equipment (STE) and KOV-14 cards are unclassified when disassociated.

(4) When the KOV-14 card is inserted into the STE, the telephone is considered classified at the designated level and requires protection by the physical presence of an individual with access equal to or higher than the classification level in accordance with Paragraph 6.2. of this Manual.

(5) List secure telephones on the SF 701 of workspaces where located. Ensure secure telephones are part of end of day security checks to ensure KOV-14 card are removed from secure phones.

(6) Direct questions regarding the proper use, operation, control, maintenance, and safeguards of secure voice telephones and accessories to the DCMA COMSEC PM.

8.6. SHIPMENT OF BULK CLASSIFIED MATERIALS.

a. DoDM 5200.01, Volume 3, Enclosure 4, provides guidance for the shipment of bulk items containing classified information as freight.

b. Commanders/Directors (or designated representatives) will notify the ISPM or DCMAS PSO (as applicable) of organizational moves involving classified information.

c. Prior to scheduling the move of large quantities of DCMA controlled classified information or equipment or unusual-sized items containing classified information, a transportation plan will be developed. Transportation plans will be:

(1) Coordinated with the DCMA Security INFOSEC team not less than 60 days prior to the planned movement.

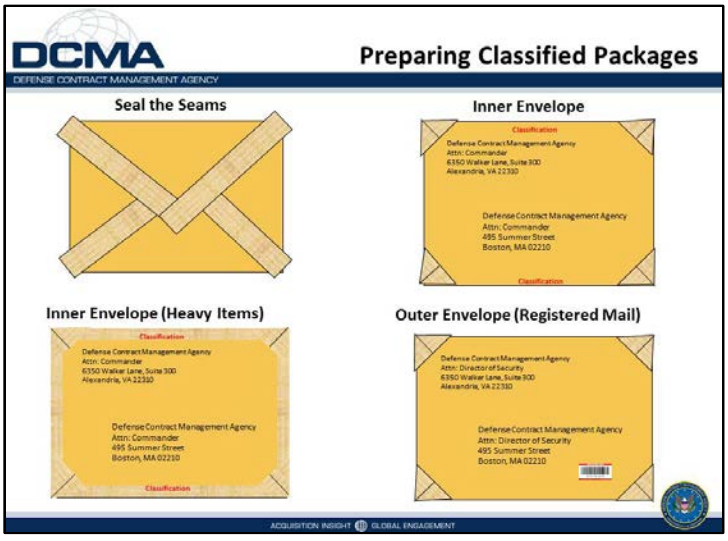
(2) Approved by the ISPM or DCMAS PSO (as applicable).

8.7. PREPARING CLASSIFIED MATERIAL FOR SHIPMENT.

a. Items containing classified information prepared for shipment will be properly packaged to deter or mitigate risk of compromise. Persons packaging or shipping items containing classified information must have validated access in accordance with Paragraph 6.2 of this Manual, to the classified information contained in the items being shipped.

b. When transferring classified information, it will be enclosed in two opaque sealed envelopes, wrappings, or containers durable enough to properly protect the information from accidental exposure and facilitate detection of tampering. Detailed guidance for the preparation, packaging, sealing, marking, and addressing of packages containing classified information is contained in DoDM 5200.01, Volume 3, Enclosure 4. This guidance will be strictly followed when preparing packages containing classified information. Figure 9 provides an illustration of a properly prepared package.

Figure 9. Classified Package Wrapping and Marking



8.8. ESCORT, COURIER, OR HAND CARRYING CLASSIFIED INFORMATION.

a. Authority to Escort or Hand-Carry Classified Information.

(1) Appropriately cleared and briefed personnel are authorized to escort or hand-carry classified material between locations when other means of transmission or transportation cannot be used. Within DCMA, the escort or hand-carry of classified material is only authorized when there is an operational necessity or a contractual requirement for the classified information at the intended destination and when all other possible means of transmission (secure e-mail, secure FAX, approved mailing/freight, or other secure methods) will not meet the mission requirement.

(2) The responsible Commander/Director with the operational requirement will serve as the approving authority for the escort or hand-carrying of classified materials. Prior to decisions to escort or hand-carry classified materials, the responsible Commander/Director (or designated representative) will coordinate the action with the ISPM or DCMAS PSO (as applicable) to ensure all other means of transmitting the information are exhausted and DoD and DCMA requirements are met.

b. Packaging Requirements. Classified materials that are to be escorted or hand-carried will be packaged in accordance with the requirements established in DoDM 5200.01, Volume 3, Enclosure 4. and Paragraph 8.7 of this Manual.

c. Designating and Approving Personnel to Escort or Hand-Carry Classified Material.

(1) The Commander/Director with the operational mission necessitating the escort or hand-carrying of classified information will select the individual(s) to act as courier. Personnel selected to perform these duties will meet the following requirements:

(a) Possess a valid security clearance equivalent to or higher than the highest classification level of the material being escorted or hand-carried in accordance with Paragraph 6.2. of this Manual.

(b) Trained in the duties and responsibilities of a courier and in the actions to take during emergencies or in the event of a loss or compromise.

(c) Possess a DoD common access card (CAC) and/or a contractor-issued identification card and a government-issued photo identification card. One of the identification cards will contain date of birth, height, weight, and signature.

(2) Once the responsible commander/director has identified an individual to act as courier, the Classified Information Courier Authorization Request Form, available on the DCMA-DCS INFOSEC resources Web page, will be completed. The Commander/Director will complete Sections I through III and sign Section III.

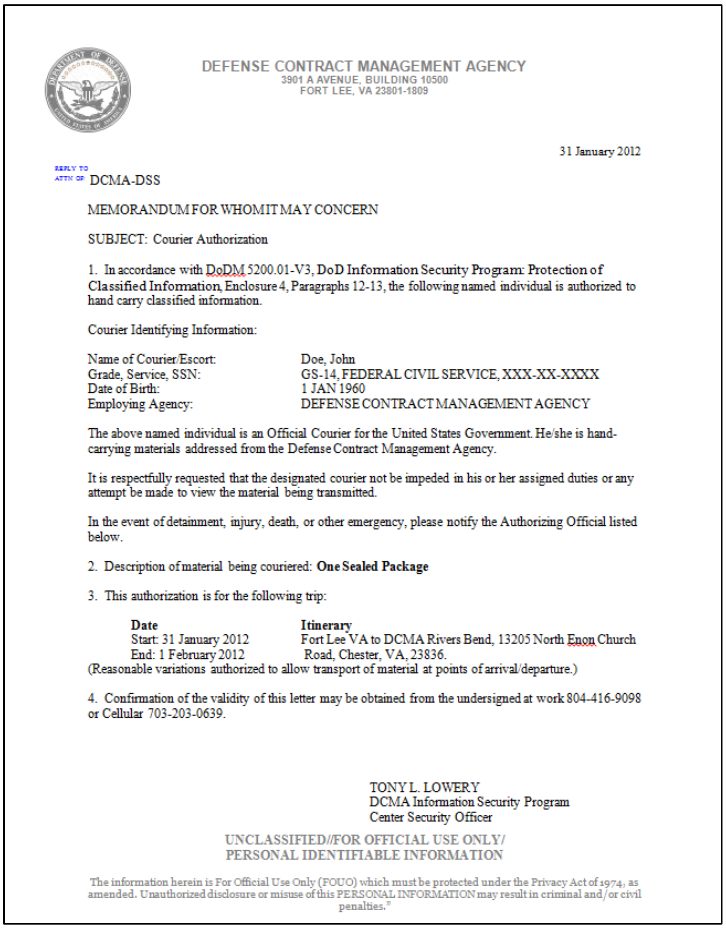
(3) The person acting as courier will then read, complete, and sign Section IV of the form. Once Sections I through IV are completed, the Classified Information Courier Authorization Request Form is forwarded to the ISPM or the DCMAS PSO (as applicable) to schedule courier training.

(4) Upon receipt of the Classified Information Courier Authorization Request Form, the ISPM, IPTL, or DCMAS PSO will schedule the courier for training. Training will meet all requirements of DoDM 5200.01, Volume 3, Enclosure 4.

(5) At the conclusion of the courier training, the approving security authority will complete Section V of the Classified Information Courier Authorization Request Form and issue the individual a courier authorization memorandum (Figure 10) or a DD Form 2501 "Courier Authorization."

(6) The DD Form 2501 is an accountable document and only issued when a demonstrated recurring need to hand-carry classified information. DD Forms 2501 will be signed by the responsible security authority. The form is valid for one year from issuance.

Figure 10. DCMA Courier Authorization Memorandum



DEFENSE CONTRACT MANAGEMENT AGENCY
3901 A AVENUE, BUILDING 10500
FORT LEE, VA 23801-1809

31 January 2012

REPLY TO ATTN OF DCMA-DSS

MEMORANDUM FOR WHOM IT MAY CONCERN

SUBJECT: Courier Authorization

1. In accordance with DoDM 5200.01-V3, DoD Information Security Program: Protection of Classified Information, Enclosure 4, Paragraphs 12-13, the following named individual is authorized to hand carry classified information.

Courier Identifying Information:

Name of Courier/Escort:	Doe, John
Grade, Service, SSN:	GS-14, FEDERAL CIVIL SERVICE, XXX-XX-XXXX
Date of Birth:	1 JAN 1960
Employing Agency:	DEFENSE CONTRACT MANAGEMENT AGENCY

The above named individual is an Official Courier for the United States Government. He/she is hand-carrying materials addressed from the Defense Contract Management Agency.

It is respectfully requested that the designated courier not be impeded in his or her assigned duties or any attempt be made to view the material being transmitted.

In the event of detainment, injury, death, or other emergency, please notify the Authorizing Official listed below.

2. Description of material being couriered: **One Sealed Package**

3. This authorization is for the following trip:

Date	**Itinerary**
Start: 31 January 2012	Fort Lee VA to DCMA Rivers Bend, 13205 North Enon Church
End: 1 February 2012	Road, Chester, VA, 23836.

(Reasonable variations authorized to allow transport of material at points of arrival/departure.)

4. Confirmation of the validity of this letter may be obtained from the undersigned at work 804-416-9098 or Cellular 703-203-0639.

TONY L. LOWERY
DCMA Information Security Program
Center Security Officer

UNCLASSIFIED//FOR OFFICIAL USE ONLY/
PERSONAL IDENTIFIABLE INFORMATION

The information herein is For Official Use Only (FOUO) which must be protected under the Privacy Act of 1974, as amended. Unauthorized disclosure or misuse of this PERSONAL INFORMATION may result in criminal and/or civil penalties.

d. Customs, Police, and Immigration Coordination. When required, the courier will ensure arrangements are made in advance with customs, police, and/or immigration officials. When such coordination is necessary, the courier will follow the guidance contained in DoDM 5200.01, Volume 3, Enclosure 4.

e. Hand-Carrying Classified Material Aboard Commercial Passenger Aircraft.

(1) Approval authority to hand-carry classified information aboard a commercial passenger aircraft within the continental United States is limited to Executive Directors, Regional, and CMO Commanders/Directors. Approving authority for the hand-carry of classified information aboard commercial passenger aircraft outside the continental United States is limited to the ISPM.

(2) Hand-carrying of classified information aboard commercial passenger aircraft, particularly overseas or to overseas destinations, is discouraged because of the potential for hijacking and the increased risk of compromise.

(3) Couriers will follow guidance in DoDM 5200.01, Volume 3, Enclosure 4, when classified information is transported aboard commercial passenger aircraft.

SECTION 9: SECURITY EDUCATION AND TRAINING

9.1. GENERAL.

a. All DCMA personnel are responsible for safeguarding classified and sensitive information. Appropriate training and awareness is required to help meet these responsibilities.

b. All DCMA civilian, military, and contractor personnel (consistent with the terms and conditions of their contract) will complete INFOSEC training on a continuous basis. Personnel will complete training consistent with their duties, responsibilities, and access to classified information and CUI.

c. Commanders/Directors will ensure personnel complete and remain current on all required INFOSEC training. Individuals failing to complete or remain current on required training will not be granted access to classified or unclassified national security information.

9.2. INITIAL ORIENTATION.

a. Initial security orientation training is designed to provide employees new to DCMA with the knowledge necessary to protect classified or unclassified national security information and their responsibilities under the INFOSEC Program.

b. All personnel new to DCMA will receive initial security orientation training by a DCMA security specialist within 90 days of assignment. DCMA-DCS security specialists will coordinate and schedule employees to complete this training. Commanders/Directors will ensure employee availability.

c. The ISPM is responsible for developing, updating, and disseminating a standardized initial security orientation training package (presentation, script, training aids, etc.) for use throughout the Agency. At a minimum, the initial security orientation will meet all requirements outlined in DoDM 5200.1, Volume 3, Enclosure 5, Paragraph 3 and will be reviewed and updated (as necessary) annually.

d. The initial security orientation training may be conducted in-person, by computer-based and instructor lead training, via video teleconference, or via telephone.

e. The ISPM and the IPTL will ensure training records (attendance rosters, etc.) are retained consistent with DCMA records management guidance to support assessment and/or inquiry/investigations processes.

9.3. INITIAL SECURITY CLEARANCE INDOCTRINATION. All personnel who require access to classified information in the performance of their duties will complete indoctrination as outlined in the DCMA-MAN 4201-07 prior to being granted access to classified information.

9.4. ORIGINAL CLASSIFICATION AUTHORITY (OCA) TRAINING.

a. Persons (DCMA Director) designated as an OCA will receive initial training prior to rendering classification decisions and annually thereafter. When classification decisions are necessary and line of succession actions are in effect and appointment orders are in place, the person acting as the DCMA Director will be trained in OCA responsibilities prior to rendering classification decisions.

b. The ISPM will develop or designate a training package to support OCA training. The OCA training will address the requirements of DoDM 5200.01, Volume 3, Enclosure 5.

c. OCA training completion will be certified in writing with training certification records retained by the ISPM in accordance with DCMA records management policy.

d. Personnel involved in the preparation of original classification recommendations will also complete OCA training. These personnel will notify the ISPM of the requirement prior to initiating any classification decision preparation work.

9.5. DERIVATIVE CLASSIFICATION TRAINING.

a. DCMA personnel will meet the requirements of Paragraph 6.2. of this Manual and be trained in the proper application of derivative classification principles prior to applying derivative classification markings. There is no specific designation required for derivative classifiers.

b. The ISPM will ensure derivative classification training is integrated into the initial and annual training curriculum completed by all DCMA personnel. This ensures all agency personnel are trained in rendering derivative classification decisions.

9.6. ANNUAL REFRESHER TRAINING.

a. All DCMA personnel will complete annual INFOSEC refresher training. This training is designed to reinforce the policies, principles, and procedures addressed in initial training.

b. Normally, annual INFOSEC training is accomplished via computer-based training. Annual INFOSEC refresher training may be presented by a member of the DCMA Security INFOSEC team via DCO or teleconference.

c. The ISPM is responsible for developing, updating, and disseminating an annual standardized INFOSEC training package (presentation, script, training aids, etc.) for use throughout the Agency. Annual refresher training will meet all requirements of DoDM 5200.01, Volume 3, Enclosure 5.

d. The responsible RIS working with Commanders/Directors (or designated representative) will monitor annual INFOSEC training completion to ensure personnel are compliant.

9.7. CONTINUING SECURITY TRAINING AND AWARENESS. INFOSEC training and awareness must be continuous, rather than a single annual security event to help influence

DCMA personnel's security performance. INFOSEC topics should be integrated into briefings, meetings, lectures, etc. to compliment formal training presentations. The following venues may be undertaken to enhance the INFOSEC competency and awareness of the workforce:

a. Large group meetings. Commanders/Directors are encouraged to include INFOSEC related topics in meetings where large groups of assigned personnel are present, such as "all hands" meetings. The supporting RIS may offer support by in-person or video-teleconferencing participation and providing training materials or awareness information.

b. Quarterly INFOSEC Awareness Presentations. Periodically, the ISPM will prepare and submit to the workforce, via headquarters messenger, short INFOSEC specific training presentations designed to enhance awareness. Presentations will cover a single topic DCMA personnel are likely to encounter in the performance of their duties or other hot topic items.

c. "The Sentinel" Newsletter. Periodically, the ISPM will include INFOSEC awareness information articles published via the DCMA security newsletter "The Sentinel."

d. Pod-Casts. Pod-casts offer a tremendous opportunity for providing training to the workforce and for highlighting areas of interest within the INFOSEC community. The ISPM and/or IPTL will coordinate topics for presentation through pod-cast with the DCMA Congressional and Public Affairs Office.

e. Security Representatives will work with supporting RIS's to obtain, post, and as necessary refresh Security Awareness and Education posters and media throughout the workplace.

9.8. TERMINATION BRIEFINGS. DCMA-MAN 4201-07 provides guidance on termination briefings.

9.9. ISPM TRAINING AND CERTIFICATION.

a. Training Requirements. The DCMA ISPM is the DCMA INFOSEC subject matter expert. As such, the ISPM must be trained in the full spectrum of INFOSEC related topics. The following list identifies the minimum training requirements for the ISPM:

(1) Instructor-Led Course. Information Security Management IF201.01.

(2) Center for Development of Security Excellence (CDSE) eLearning Courses:

- Risk Management for DoD Security Programs GS102.16
- Classification Conflicts and Evaluations IF110.16
- Derivative Classification IF103.16
- Information Security Emergency Planning IF108.06
- Introduction to Information Security IF011.16
- Marking Classified Information IF105.16
- Original Classification IF102.16
- Personally Identifiable Information (PII) DS-IF101.06

- Phishing DS-IA103.06
- Security Classification Guidance IF101.16
- Transmission and Transportation for DoD IF107.16
- DISAM - International Programs Security Requirements IPSR-OLL IN112.06
- Introduction to Industrial Security IS011.16
- Introduction to Personnel Security PS113.16
- Storage Containers and Facilities PY105.16
- SAP Overview SA001.16

(3) Defense Information Security Agency Course. Information Assurance for Professionals Shorts.

(4) National Counterintelligence Executive Courses:

- General Security
- Unauthorized Disclosures of Classified Information
- Classification Management

b. Certification Requirements.

(1) The ISPM will be certified under the Defense Security Professional Certification Program as outlined in DoDI 3305.13, "DoD Security Training." Required certifications for the ISPM are as follows:

- Security Fundamentals Professional Certification (SFPC)
- Security Asset Protection Professional Certification (SAPPC)
- Security Program Integration Professional Certification (SPIPC)

(2) New hires into the ISPM position will obtain certification within 2 years of appointment as a condition of employment. Once obtained, the SPIPC will be maintained in accordance with DoDI 3305.13.

9.10. SECURITY SPECIALIST TRAINING AND CERTIFICATION.

a. Training Requirements. RIS's are advisors to Commanders/Directors in the field and lead INFOSEC program efforts within assigned regions. As such, RISs must be trained sufficiently to perform the duties and responsibilities assigned to them. The minimum training requirements for the RISs are as follow:

(1) Center for Development of Security Excellence (CDSE) eLearning Courses:

- Risk Management for DoD Security Programs GS102.16
- Classification Conflicts and Evaluations IF110.16
- Derivative Classification IF103.16
- Information Security Emergency Planning IF108.06

- Introduction to Information Security IF011.16
- Marking Classified Information IF105.16
- Original Classification IF102.16
- Personally Identifiable Information (PII) DS-IF101.06
- Phishing DS-IA103.06
- Security Classification Guidance IF101.16
- Transmission and Transportation for DoD IF107.16
- DISAM - International Programs Security Requirements IPSR-OLL IN112.06
- Introduction to Industrial Security IS011.16
- Introduction to Personnel Security PS113.16
- Storage Containers and Facilities PY105.16
- SAP Overview SA001.16

(2) Defense Information Security Agency Course. Information Assurance for Professionals Shorts.

(3) National Counterintelligence Executive Courses.

- General Security
- Unauthorized Disclosures of Classified Information
- Classification Management

b. Certification Requirements.

(1) The regional INFOSEC specialists and other security specialists with information security responsibilities will be certified under the Defense Security Professional Certification Program outlined in DoDI 3305.13. Required certifications for these personnel are as follows:

- Security Fundamentals Professional Certification (SFPC)
- Security Asset Protection Professional Certification (SAPPC)

(2) New hires into security specialist positions will obtain certification within 2 years of appointment as a condition of employment. Once obtained, the SAPPC will be maintained in accordance with DoDI 3305.13. The ISPM and Executive Director, DCMAS (as applicable) will ensure position descriptions are updated (as necessary) to reflect this DoD level requirement.

9.11. SECURITY REPRESENTATIVE TRAINING. Security representatives are a vital part of the organization's overall security apparatus. Training must provide the necessary understanding and skills to manage security programs at the organizational level. Initial training for security representatives will be developed, fielded, and reviewed on an annual basis to ensure currency. Refer to DCMA-INST 1091 concerning security representative/specialist training requirements relating to SAPs.

(1) Supporting RIS will coordinate and provide initial training to newly appointed security representatives within 60 days of appointment. The initial training will be broad in

scope concerning the overall DCMA INFOSEC Program. Training to address skills associated with recognizing classified information, actions to take during security incidents, management of security containers, and other daily tasks will consist of enough detail to help security representatives to perform the duties and responsibilities assigned to them.

(2) All security representatives will receive recurring training at least semiannually provided by the supporting RIS. The recurring training is intended to be as short as possible to remind security representatives of their responsibilities and any changes to INFOSEC or associated policy or procedures.

(3) Security representatives should participate in online training provided by the CDSE related to INFOSEC duties.

SECTION 10: SECURITY INCIDENTS

10.1. GENERAL.

a. Protection of classified information and CUI is essential to maintaining security and achieving mission success in DoD's operational environments. Prompt reporting of security incidents ensure incidents are properly investigated and necessary actions are taken to negate or minimize risks of loss or compromise of classified information. Security incidents involving CUI are addressed in Section 11 of this Manual.

(1) Security Infraction. A security infraction is an incident involving failure to comply with requirements of this Manual or other applicable DoD policy not resulting in the loss, suspected or actual compromise of classified information or CUI. While infractions do not constitute a security violation, if left uncorrected they can lead to security violations or compromises of information. A preliminary inquiry will be conducted when a security infraction is suspected. The inquiry will focus on the root causes of the circumstances leading to the infraction and will identify appropriate corrective actions.

(2) Security Violation. A security violation is any incident that results in, or could be expected to result in, the loss or compromise of classified information or CUI; to include the willful disregard of security regulations and policies. Security violations require a preliminary inquiry and/or formal investigation based on the severity of the compromise and/or the level of classified information involved.

(a) Compromise. A compromise is a security violation where an unauthorized disclosure of classified information (i.e., disclosure to a person(s) who does not have a valid clearance, authorized access, or a need to know) occurred. A compromise involving CUI is the disclosure of the information to person(s) without a valid need to know.

(b) Loss. A loss occurs when classified information or CUI cannot be physically located or accountability is not maintained (e.g., items or equipment containing classified information is discovered missing during an audit and cannot be immediately located).

b. Preliminary Inquiry (PI). A PI is a fact-finding and analysis process conducted to determine if a loss of classified information or CUI occurred, or if unauthorized personnel had, or could have had, access to classified information or CUI, or if either circumstance cannot be ruled out. The PI:

- Identifies the facts surrounding the incident
- Characterizes the incident as an infraction or a violation
- Identifies, if possible, the cause(s) and person(s) responsible for causing the incident
- Reports corrective actions taken or to be taken
- Makes recommendations as to the need for corrective action or an investigation

b. Investigation. An investigation is conducted on security incidents when the incident cannot be resolved by a PI or for incidents where an in-depth and comprehensive examination of

the matter is appropriate. Investigations will be initiated if DCMA personnel (military, civilian, or contractor) knowingly, willfully, or negligently:

- Disclose to unauthorized persons information properly classified under E.O. 13526.
- Create or continue a SAP contrary to the requirements of applicable DoD policies.
- Commit repeated administrative discrepancies that do not subject classified information to loss or compromise, but indicate a disregard or malice for security procedures.
- Copy, scan, or transmit classified information through unclassified computer networks or systems.

c. Command Responsibility. The Commander/Director with security responsibility for the information involved in security incidents will ensure a PI or formal security investigation is conducted based on the guidance contained in Paragraph 10.5. of this Manual and DCMA "DCMA Information Security Handbook for Preliminary Inquiry and Investigations," which may be obtained from the DCMA Security INFOSEC resource page.

10.2. REPORTING AND NOTIFICATIONS.

a. General.

(1) The prompt reporting of actual or suspected security incidents ensures containment of the incident, reduces further compromise of classified information, and timely notification of appropriate authorities.

(2) Within DCMA, actual or suspected security incident reporting requirements are contained in DoDM 5200.01, Volume 3, Enclosure 6 and Paragraph 10.2.c. of this Manual.

b. Internal (DCMA) Reporting Requirements.

(1) DCMA employees (civilian, military, or contractor) who find classified information out of proper control will take custody of the information, safeguard it, and promptly notify their management of the incident. When available, secure communications will be used to report the incident; however, notification will not be delayed due to secure communications are not readily available.

(a) Upon notification of a security incident, the responsible Commander/ Director or Manager will promptly notify the DCMA INFOSEC team (RIS, IPTL, or ISPM for non-DCMAS incidents or the PSO for DCMAS incidents) and their operational chain of command.

(b) The responsible security official will immediately gather information to determine if the security incident can be confirmed and if the incident is likely to become public. Upon confirmation of the incident or if there is reason to believe the incident will become public, immediately notify the ISPM. The ISPM will accomplish the reporting requirements in Paragraph 10.2.c. of this Manual.

(c) Immediately report incidents involving SAP and/or SCI to the DCMAS PSO and SSO, refer to DCMA-INST 1091.

c. Security Incidents Requiring OSD Notification.

(1) The ISPM will promptly notify the DSCI and the OUSD(I), of all confirmed security incidents having significant consequences or may become public.

(2) DoDM 5200.01, Volume 3, Enclosure 6 provides specific guidance regarding incidents requiring prompt notification of the OSD in accordance with Paragraph 10.2.b.(1)(b), of this Manual.

(3) The ISPM will promptly notify the Deputy Under Secretary of Defense for Intelligence and Security (DUSD(PI)) of all violations involving SAP, NATO or FGI.

(4) The Executive Director, DCMAS will ensure any SAP specific reporting requirements are accomplished.

10.3. CLASSIFICATION OF SECURITY INCIDENT REPORTS. DoDM 5200.01, Volume 3, Enclosure 6 provides detailed guidance regarding classifying and markings security incident reports.

10.4. SPECIAL CIRCUMSTANCES/CONSIDERATIONS.

a. Security Incidents Involving a Deliberate Compromise to a Foreign Intelligence Service or Terrorist Organization. Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

b. Security Incidents Involving Apparent Violations of Criminal Law. Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

c. Security Incidents Involving COMSEC or Cryptographic Information. DCMA-MAN 3301-09, addresses COMSEC reporting requirements.

d. Security Incidents involving SCI. Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

e. Security Incidents Involving RD or FRD. Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

f. Security Incidents involving IT.

(1) Within DCMA, the most common security incident involving IT is a computer spillage. Computer spillage occurs when classified information or other restricted information is introduced into a non-classified IT system. Actual or potential compromises of classified

information involving automated information systems or computer systems, terminals, or equipment require immediate action to contain the situation and prevent further unauthorized disclosures. All actual or suspected computer spillage will be promptly reported to the DCMA Network Operations Center (NOSC) at **678-626.4422**. In addition to NOSC notification, personnel involved in a computer spillage will accomplish the following:

- Disconnect the computer from the network (do not turn off/power down the computer until instructed) and ensure affected computers are secured
- Disconnect the device(s) from the network to include peripheral devices if they were used to print, copy, or scan documents
- Follow the guidance issued by NOSC personnel
- If the computer spillage occurs as a result of information received from another party, promptly notify the person sending the information, by means other than the affected e-mail system, of the actual or suspected computer spillage
- Immediately notify other recipients of the e-mail by some other means than e-mail

(2) Contact DCMAS if SAP or SCI is involved for further direction.

(3) Local information assurance (IA) officials will initiate immediate technical support, as directed by the NOSC, to bring prompt resolution to incidents.

(4) The responsible Commanders/Directors will ensure personnel and other resources (computer, etc.) are made immediately available so that the incident can be quickly contained and further compromise limited.

(5) Other IT-related considerations are contained in DoDM 5200.01, Volume 3, Enclosure 6.

g. Security Incidents Involving FGI or NATO Information. Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

h. Security Incidents Involving Classified U.S. Information Provided to Foreign Governments. Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

i. Security Incidents Involving SAPs. Reporting and handling requirements for these types of incidents are covered in DCMA-INST 1091.

j. Security Incidents Involving Improper Transfer of Classified Information. Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

k. Security Incidents Involving On-Site Contractors.

(1) Security incidents, including any inquiries or investigations, involving on-site contractors will be handled in accordance with Paragraph C1-303 of DoD 5220.22-R, "Industrial Security Regulation." The contractor's security manager must ensure the DCMA ISPM receives copies of any reports pertaining to incidents involving DCMA associated classified information or CUI. These reports must be received by the ISPM within 15 days of completion of the inquiry or investigation.

(2) The corporate employer of the individual contractor involved in the incident is responsible for disciplinary action and/or sanctions unless specifically addressed in the contract.

(3) DCMA retains the ability, when appropriate and in accordance with the authorities and requirements of DoD 5220.22-R, to deny access to classified information and to take other administrative actions as deemed necessary or appropriate.

l. Security Incidents Involving Critical Program Information (CPI). Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

m. Security Incidents Involving ACCM-Protected Information. Reporting and handling requirements for these types of incidents are covered under DoDM 5200.01, Volume 3, Enclosure 6.

n. Absence without Authorization. Reporting and handling requirements for this type of incident are covered under DoDM 5200.01, Volume 3, Enclosure 6.

o. Coordination with Legal Counsel and Department of Justice (DOJ). Reporting and handling requirements concerning unauthorized disclosure of classified information via the media are covered under DoDM 5200.01, Volume 3, Enclosure 6, and Appendix 2.

p. Insider Threat. Reporting and handling requirements for incidents with an Insider Threat nexus are covered under DCMA-MAN 3301-05, "Insider Threat Program."

10.5. CONDUCTING PRELIMINARY INQUIRES AND INVESTIGATIONS.

a. All known or suspected instances of unauthorized disclosure of classified information will be promptly reported to the ISPM or DCMAS PSO (as applicable). The ISPM or DCMAS PSO (as applicable) will determine if the need exists for a PI or an investigation.

b. Should it be determined that a PI or investigation is required, the responsible Commander/Director will initiate the inquiry/investigation to determine the facts and circumstances surrounding the incident.

c. Once notified of a requirement to conduct an inquiry/investigation, the responsible Commander/Director will, within 2 duty days of notification, appoint in writing a disinterested official to conduct the inquiry/investigation. Once appointed, the inquiry/investigation should be the primary duties of the investigating official. Inquiries/investigations into actual or suspected

compromises of classified information will not be delayed due to temporary duty (TDY) or leave. Persons appointed to serve as an investigating official will meet the following requirements:

(1) Possess a security clearance and access equal to or higher than the highest classification of the information affected by the incident.

(2) Be an officer, senior noncommissioned officer, or DoD civilian (general schedule (GS)-9 or above) and of a higher grade than the persons suspected of causing the incident.

(3) Not serve as security representatives or the supporting security official as these individuals have defined security responsibilities that may come under scrutiny during the inquiry/investigation.

(4) Not be assigned to the same office to prevent possible allegations of biased reporting.

10.6. INFORMATION APPEARING IN THE PUBLIC MEDIA.

a. If classified information appears in the public media (including on public internet sites) or if approached by a representative of the media, DCMA personnel will be careful not to make any statement or comment confirming the accuracy or verifying the information requiring protection.

b. All such situations will be promptly reported to the ISPM for guidance and to meet reporting requirements outlined in Paragraph 10.2. of this Manual.

c. Detailed guidance regarding the handling and reporting of incidents where classified information appears in the public domain is outlined in DoDM 5200.01, Volume 3, Enclosure 6.

10.7. DAMAGE ASSESSMENTS.

a. A damage assessment is an analysis to determine the effect of a compromise of classified information on the national security.

b. Most violations that involve DCMA personnel concern other military department or DoD agency information. In instances where the information belongs to an OCA other than the DCMA OCA, the ISPM or DCMAS PSO (as applicable) will ensure the incident is reported to the affected OCA.

c. Upon notification of an actual or suspected compromise, the OCA is responsible for conducting a damage assessment. DCMA will assist the OCA in the damage assessment.

d. Additional guidance involving the conduct of damage assessments is contained in DoDM 5200.01, Volume 3, Enclosure 6.

10.8. INADVERTENT DISCLOSURE DEBRIEFING REQUIREMENTS.

a. In cases where unauthorized access to classified information has occurred, the ISPM or DCMAS PSO (as applicable) will determine if a debriefing is warranted. This decision will be based on the circumstances of the incident, what is known about the person(s) involved, and the nature of the information. The following general guidelines apply:

(1) If the unauthorized access was by a person with the appropriate security clearance but no need to know, debriefing is appropriate to ensure that the individual is aware the information to which they had unauthorized access is classified and requires protection.

(2) If the unauthorized access was by U.S. Government civilian or military personnel or an employee of a U.S. Government contractor who does not have a security clearance, debriefing is appropriate and the following actions will be accomplished.

(a) The person will be advised of his or her responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if they fail to do so.

(b) The debriefing will be designed to ensure the individual understands the nature of the information, why its protection is important, and guidance on what to do if someone tries to obtain the information.

(c) In the case of non-DoD U.S. Government personnel and employees of U.S. Government contractors, the appropriate security official in the individual's parent organization, including the appropriate facility security officer where applicable, will be advised of the debriefing.

b. When an inadvertent disclosure debriefing is conducted, an inadvertent disclosure statement (Figure 11) will be completed and filed with any final reports of investigation or inquiry.

10.9. CORRECTIVE ACTIONS AND SANCTIONS.

a. Commanders/Directors must ensure prompt and appropriate management action is taken in cases of confirmed compromises of classified information, improper classification of information, violations of the provisions of this instruction, and incidents that may put classified information at risk of compromise. Corrective actions will focus on correcting or eliminating the conditions that caused the incident.

b. When deemed appropriate, Commanders/Directors may consider sanctions to address the incident. Sanctions might include warnings, reprimands, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of classification authority. Action may also be taken under the Uniform Code of Military Justice and under applicable criminal law.

c. Any proposed action to sanction a DCMA civilian employee will be coordinated with the Human Capital Directorate and the Office of General Counsel. Any proposed action against

DCMA military personnel will be coordinated with the HQ DCMA Military Personnel Office and the responsible General Counsel. The DCMA PERSEC Program will be consulted when considering suspension or revocation of an individual's security clearance.

Figure 11. DCMA Inadvertent Disclosure Statement

INADVERTENT DISCLOSURE BRIEFING

1. Information of a classified nature has been either discussed with you or exposed to your view. This disclosure was unintentional. It is therefore necessary to acquaint you with the law on this subject and for you to execute a statement binding you to secrecy in connection with any information you may have gained from this disclosure.

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

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

INADVERTENT DISCLOSURE AGREEMENT

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

_____ _____

Printed Name Date

_____ _____

Signature Last 4 Social Security Number

SECTION 11: IDENTIFICATION AND PROTECTION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI)

11.1. GENERAL.

a. In addition to classified information, certain types of unclassified information require access and distribution controls and other protective measures. Such information is referred to collectively as CUI as required by E.O. 13556. This section identifies the controls and protective measures required for CUI.

b. In accordance with E.O. 13556, information may not be designated CUI to:

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a person, organization, or agency
- Restrain competition
- Prevent or delay the release of information that does not require protection under statute or regulation

c. The originator of a document is responsible for determining at origination whether the information contained therein qualifies for CUI status, and if so, for applying the appropriate CUI markings. However, this responsibility does not preclude competent authority (e.g., officials higher in chain of command or functional experts) from modifying existing markings or adding additional markings. In such cases, the originator will be notified of any changes to the original decision or markings.

d. All DoD unclassified information must be reviewed and approved for release through standard DCMA processes before it is provided to the public (including via posting to publicly accessible websites) in accordance with DoDD 5230.09, Deputy Secretary of Defense Memorandum, "Web Site Administration," (with attachments) and other applicable regulations.

11.2. FOR OFFICIAL USE ONLY (FOUO).

a. Dissemination Exemption. FOUO is a dissemination control applied by DoD to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more exemptions of the Freedom of Information Act (FOIA) (Section 552 of Title 5, United States Code.

b. Access to FOUO Information.

(1) No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.

(2) The final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge, or control of the information and not on the prospective recipient.

(3) Information designated as FOUO may be disseminated within DoD components and between officials of DoD components and DoD contractors, consultants, and grantees to conduct official business for the DoD, provided that dissemination is not further controlled by a distribution statement.

(4) DCMA holders of information designated as FOUO are authorized to convey such information to officials in other departments and agencies of the executive and judicial branches to fulfill a Government function. If the information is covered by the Privacy Act, disclosure is only authorized if the requirements of DoD 5400.11-R, "DoD Privacy Program" are also satisfied.

(5) DoDI 7650.01, "Government Accountability Office (GAO) and Comptroller General Requests for Access to Records" governs release of FOUO information to the GAO. If the Privacy Act covers the information, disclosure is authorized if the requirements of DoD 5400.11-R, are also satisfied.

c. Protection of FOUO Information.

(1) During working hours, reasonable steps will be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving FOUO information unattended where unauthorized personnel are present).

(2) After working hours, FOUO information may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided. If such building security is not provided or is deemed inadequate, the information will be stored in locked desks, file cabinets, bookcases, locked rooms, etc.

(3) FOUO information may be transmitted via first class mail, parcel post, or, for bulk shipments, via fourth class mail. Whenever practical, electronic transmission of FOUO information (e.g., data, Web site, or e-mail) will be by approved secure communications systems or systems utilizing other protective measures such as public key infrastructure (PKI) (encrypted) or transport layer security (e.g., https). Transmission of FOUO by FAX machine is permitted; however, the sender is responsible for determining that appropriate protection will be available at the receiving location prior to transmission (e.g., machine attended by a person authorized to receive FOUO, FAX located in a controlled Government environment).

d. Marking FOUO.

(1) Information that has been determined to qualify for FOUO status will be indicated by markings. Markings are to be applied at the time documents are created to properly protect the information. When a classified document or portion thereof is declassified, FOUO markings may be applied, if applicable, to protect the information.

(2) Unclassified documents and material, including information in electronic form, containing FOUO information will be marked as follows:

(a) Each document determined to contain FOUO information will identify the originating agency or office. This information will be clear and complete enough to allow someone receiving the document to contact the office if questions or problems about the designation or markings arise.

(b) Documents will be marked "FOR OFFICIAL USE ONLY" at the bottom of the outside of the front cover (if there is one), the title page, the first page, and the outside of the back cover (if there is one). Optionally, for consistency with classified systems, the document may be marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY."

(c) Internal pages of the document that contain FOUO information will be marked "FOR OFFICIAL USE ONLY" at the bottom. Optionally, for consistency with classified systems, internal pages may be marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" or "UNCLASSIFIED//FOUO;" in such case internal pages will be marked at both the top and bottom.

(d) Subjects, titles, and each section, part, Paragraph, or similar portion of an FOUO document will be marked to show that they contain information requiring protection. Use the parenthetical notation "(FOUO)" (or optionally "(U//FOUO)") to identify information as FOUO for this purpose. Place this notation immediately before the text.

(e) Each part of electronically transmitted messages, including mail, containing FOUO information will be marked as required by DoDM 5200.01, Volume 4, Enclosure 3, Paragraph 2.c. Unclassified messages containing FOUO information will be marked "FOR OFFICIAL USE ONLY" (optionally "UNCLASSIFIED//FOR OFFICIAL USE ONLY" or "UNCLASSIFIED//FOUO") before the beginning of the text and will contain the parenthetical portion marking "(FOUO)" (optionally "(U//FOUO)") at the beginning of each portion containing FOUO information.

(f) Transmittal documents that have FOUO attachments, but no classified material attached, will be marked with the following statement "FOR OFFICIAL USE ONLY ATTACHMENT."

(g) When FOUO information is contained in media or material (including hardware and equipment) not commonly thought of as documents (e.g., computer files and other electronic media, audiovisual media, charts, maps, films, sound recordings), the requirement remains to identify, as clearly as possible, the information requiring protection. The main concern is holders and users are clearly notified of the presence of the FOUO information. The markings required by this enclosure will be applied either on the item or the documentation that accompanies it.

e. Unauthorized Disclosure. Unauthorized disclosure of FOUO information or materials does not constitute an unauthorized disclosure of DoD classified information. However, appropriate administrative action will be taken to fix responsibility for unauthorized disclosure of FOUO whenever feasible and appropriate disciplinary action will be taken against those responsible. Unauthorized disclosure of FOUO information protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The Military Department or other DoD component originating the FOUO information will be informed of its unauthorized disclosure.

f. Destruction of FOUO.

(1) Documents containing FOUO information will be destroyed by use of level 3 or 4, medium security, cross-cut (or higher level) paper shredders. An on-site shred service, approved by the ISPM, may be used in lieu of shredders.

(2) Contact your RIS to assist in identifying assets that can be used for the destruction of CUI information. The use of other means for the destruction of FOUO must be coordinated with the supporting RIS and approved by the ISPM. Paragraph 6.13. of this Manual provides guidance for acquiring destruction devices and services.

11.3. UNCLASSIFIED NAVAL NUCLEAR PROGRAM INFORMATION (U/NNPI).

a. U/NNPI is unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities. Personnel handling or controlling information or materials designated U/NNPI will follow the guidance contained in the Office of the Chief of Naval Operations Instruction (OPNAVINST) N9210.3, "Safeguarding of Naval Nuclear Propulsion Information."

b. U/NNPI will be safeguarded to prevent its disclosure to the public and others without appropriate clearance (for classified NNPI) and a need-to-know. Whenever a sentence, paragraph, document, file, photograph, audiovisual or electronic/IT media, or component contains or otherwise reveals at least one instance or an association of the following three elements, it is NNPI:

(1) A naval nuclear propulsion plant or support facility application is directly referred to by any of the following:

- Ship name or hull number
- Project designator
- Ship system identification
- Component nameplate data
- Component name revealing a reactor plant function

(2) A system or component listed in Table 2 of OPNAVINST N9210.3.

(3) Details on technical parameters or operational conditions (e.g., design temperature or pressure).

c. U/NNPI Control Officer (NNPICO). Each DCMA organization routinely dealing with NNPI will designate a manager familiar with NNPI protection procedures as the NNPICO. The NNPICO will be technically qualified or will have access to a technically qualified individual for consultation, as needed. The NNPICO will ensure appropriate measures are established and enforced to prevent unauthorized access or dissemination of NNPI.

d. Handling Requirements.

(1) Control and Storage. U-NNPI will be controlled so individuals without a need-to-know cannot obtain visual or physical access, which would permit detailed examination.

(2) Electronic Transmission. Transmission of NNPI is **prohibited** from introduction into any DCMA computing asset. Transmission of NNPI by unencrypted, uncontrolled computer networks is considered to be release to the public.

(3) Destruction. All NNPI paper documents will be destroyed by shredding. Only equipment listed on the NSA/CSS EPL for high-security crosscut paper shredders (level 5 or 6) will be used to destroy NNPI. Destruction of hardware or other computer media (CD, USB drives, hard drives etc.) containing NNPI will be conducted in the same manner as hardware or other computer media containing classified information. Contact the supporting RIS for assistance with NNPI destruction.

(4) U/NNPI Outside of the Office. U/NNPI will not be introduced to personally owned electronic equipment, media, or duplicated in a residential environment. U/NNPI documents must be returned to the work place for copying, long-term storage, and/or destruction on the user's next normal work day. All U/NNPI information must be transported per OPNAVINST N9210.3.

11.4. OTHER TYPES OF CUI.

a. Law Enforcement Sensitive (LES). LES is a marking sometimes applied, in addition to the marking "FOR OFFICIAL USE ONLY," by the DOJ and other activities in the law enforcement community, including those within the DoD. It denotes that the information was compiled for law enforcement purposes and should be afforded security in order to protect certain legitimate Government interests. Within DoD, LES information will be safeguarded and destroyed as required for FOUO information.

b. DoD Unclassified Controlled Nuclear Information (UCNI). UCNI is unclassified information regarding the security measures (including security plans, procedures, and equipment) for the physical protection of DoD special nuclear material (SNM), SNM equipment, SNM facilities, or nuclear weapons in DoD custody. Information is designated DoD UCNI in accordance with DoDI 5210.83, "Department of Defense Unclassified Controlled Nuclear

Information (DoD UCNI)" only when it is determined its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody.

c. Limited Distribution. Limited distribution is a caveat used by the National Geospatial-Intelligence Agency (NGA) to identify a select group of sensitive, unclassified imagery or geospatial information and data created or distributed by NGA or information, data, and products derived from such information. DoDI 5030.59, "National Geospatial-Intelligence Agency (NGA) LIMITED DISTRIBUTION, Geospatial Intelligence," contains details of policies and procedures regarding use of the "LIMITED DISTRIBUTION" marking.

d. Department of State (DoS) Sensitive But Unclassified (SBU) Information. DoS SBU information is information originated within the DoS which that agency believes warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure in accordance with the provisions of the FOIA. Within the DoD, DoS SBU information will be protected as required for FOUO information.

e. Drug Enforcement Administration (DEA) Sensitive Information. DEA sensitive information is unclassified information the DEA originates and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. The administrator and certain other officials of the DEA are authorized to designate information as DEA sensitive; the DoD agreed to implement protective measures for DEA sensitive information in its possession.

f. Foreign Government Information (FGI). FGI is information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation the information, the source of the information, or both, are to be held in confidence. Information produced by the U.S. Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring the information, the arrangement, or both, are to be held in confidence.

g. Personally Identifiable Information (PII). PII is information about an individual that identifies, links, relates, or is unique to, or describes them (e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc.). PII is covered by the Privacy Act of 1974 and as such disclosure and safeguarding requirements must be in accordance with DoD 5400.11-R. Questions concerning the identification, control, and handling of PII within DCMA can be directed to DCMA Privacy Officer.

SECTION 12: SECURITY ASSESSMENTS

12.1. GENERAL.

a. DCMA's unique mission and global perspective requires the Agency and its workforce to operate in a variety of locations and environments. Due to this unique operational condition, it is necessary to establish a baseline framework by which security services and support are provided to DCMA activities at all levels of the organization. One of the primary ways to ensure this support is through security assessments.

b. Security assessment guidance relating to special programs activities is located in DCMA-INST 1091.

c. The guidance, processes, and benchmarks established in the DCMA Security Site Assessment Guide, located on the Resource Page, will be used to conduct INFOSEC assessments.

12.2. SELF-ASSESSMENTS.

a. Commanders/Directors will establish and maintain a self-assessment program based on DCMA's INFOSEC Program requirements and their degree of involvement with classified information or CUI. The purpose of the self-assessment program is to evaluate the effectiveness and efficiency of the local INFOSEC program.

b. On an annual basis, Commanders/Directors will conduct an INFOSEC self-assessment on all primary and streamlined CMO headquarters and on all other locations where classified information is processed or stored. The INFOSEC benchmarks contained in the DCMA Security Site Assessment Guide, will be used to guide the self-assessment process. A report documenting the results of the self-assessment will be forwarded to the supporting RIS no later than the last business day of August each year.

c. Upon receipt of annual self-assessment reports, the RIS will consolidate the information and submit a report to the IPTL not later than the last business day of September each year. The information derived from the consolidation process will be used to identify any negative trends, identify and program for INFOSEC resources, and to highlight positive processes or practices.

d. Annually, not later than the last business day of October, the IPTL will submit a consolidated report of annual assessments to the ISPM for consideration in the annual INFOSEC program review.

12.3. FORMAL ASSESSMENTS.

a. The DCMA Security INFOSEC team will conduct formal site assessments of DCMA organizations as outlined in the DCMA Security Site Assessment Guide.

b. Formal INFOSEC assessments will consist f a review of security procedures and practices, including, but not limited to, derivative classification, dissemination, reproduction, transmission, control and accountability, storage, downgrading, declassification, destruction, and security education and training. The INFOSEC benchmarks contained in the DCMA Security Site Assessment Guide will be used to guide the assessment process.

12.4. ASSESSMENT REPORTS.

a. After each assessment, the responsible RIS will prepare and submit to the DSCI a report of findings (with recommended corrective actions) for review and approval. Once approved and signed by the DSCI, a copy of the report will be provided to the responsible Commander/ Director, security representative, and a copy will be retained by the supporting RIS.

b. Assessment reports will be marked "Unclassified//For Official Use Only (U//FOUO)" at a minimum.

GLOSSARY

G.1. ACRONYMS.

ACCM	alternative compensatory control measures
APACS	Automated Personnel Access Control System
CD	compact discs
CDSE	Center for Development of Security Excellence
CMO	contract management office
COMSEC	communications security
CSS	Central Security Service
CUI	controlled unclassified information
DAA	designated approving authority
DD Form 254	contract security classification specification
DD Form 2501	courier authorization
DCMA-INST	DCMA Instruction
DCMA-MAN	DCMA Manual
DCMAS	Executive Director, Special Programs
DCO	Defense Connect Online
DEA	Drug Enforcement Administration
DIA	Defense Intelligence Agency
DLA	Defense Logistics Agency
DNI	Director National Intelligence
DOAC	DTIC online access controlled
DOJ	Department of Justice
DOS	Department of State
DSCI	Director, Security and Counterintelligence
DTIC	Defense Technical Information Center
DVD	digital versatile discs
E.O.	executive order
EPL	evaluated products list
FAX	facsimiles
FGI	foreign government information
FOIA	Freedom of Information Act
FOUO	for official use only
FRD	formally restricted data
GAO	Government Accountability Office
GC	General Counsel
GSA	General Services Administration
HVAC	heating, ventilation, and air conditioning
HVSACO	handle via special access channels only

ICD	intelligence community directive
ICS	intelligence community technical specifications
IDS	intrusion detection system
INFOSEC	information security
Intelink	intelligence link
IPS	information processing systems
IPTL	INFOSEC program team lead
ISPM	information security program manager
IT	information technology
JPAS	Joint Personnel Adjudication System
LES	law enforcement sensitive
MFR	memorandum for record
NATO	North Atlantic Treaty Organization
NDA	non-disclosure agreement
NGA	National Geospatial-Intelligence Agency
NNPI	naval nuclear propulsion information
NOFORN	not releasable to foreign nationals
NOSC	Network Operations and Security Center
NSA	National Security Agency
OCA	original classification authority
OPNAVINST	Office of the Chief of Naval Operations Instruction
OPSEC	operations security
OSD	Secretary of Defense
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
PED	personal electronic devices
PERSEC	personnel security
PI	preliminary inquiry
PII	personally identifiable information
PM	program manager
PPBE	planning, programming, budget and execution
PSO	program security officer
RD	restricted data
RIS	regional INFOSEC specialist
SAO	senior agency official
SAP	special access program
SAPF	special access program facilities
SAPPC	Security Asset Protection Professional Certification
SBU	sensitive but unclassified
SCG	security classification guide
SCI	sensitive compartmented information

SCIF	sensitive compartmented information facility
SF	standard form
SF 700	security container information
SF 701	activity security checklist
SF 702	security container checksheet
SF 703	top secret (cover sheet)
SF 704	secret (cover sheet)
SF 705	confidential (cover sheet)
SF 706	top secret (label)
SF 707	secret (label)
SF 708	confidential (label)
SF 710	unclassified (label)
SFPC	Security Fundamentals Professional Certification
SIPRNet	secret internet protocol router network
SMO	security management office
SPIPC	Security Program Integration Professional Certification
SSO	special security officer
STC	sound transmission class
STE	secure terminal equipment
TSCO	top secret control officer
U/NNPI	unclassified naval nuclear propulsion information
UCNI	unclassified controlled nuclear information
URL	uniform resource locator
USB	universal serial bus

REFERENCES

Assistant Secretary of Defense Memorandum, "Granting of Original Classification Authority," July 11, 2000
Code of Federal Regulation, Title 32
DCMA Information Security, "Handbook for Preliminary Inquiry and Investigations"
DCMA Instruction 710, "Managers' Internal Control Program," September 12, 2011, as amended
DCMA Instruction 1091, "Special Access Security,' July 1, 2014
DCMA Manual 4501-02, "Correspondence Program,"
DCMA Manual 3301-09, "Communications Security,"
DCMA Manual 4201-07, "Personnel Security,"
DCMA Manual 4201-19, "Foreign Visits and Assignments"
DCMA Security Site Assessment Guide, September 2010
Deputy Secretary of Defense Memorandum, "Web Site Administration," December 7, 1998, with attached "Web Site Administration Policies and Procedures," November 25, 1998
DoD 5220.22-Manual, "National Industrial Security Program Operating Manual (NISPOM)," May 18 2016
DoD 5220.22-Regulation, "Industrial Security Regulation," December 4, 1985
DoD 5400.11-Regulation, "DoD Privacy Program," May 14, 2007
DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013
DoD Directive 5230.09, "Clearance of DoD Information for Public Release," April 14 2017
DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
DoD Directive 5230.24, Distribution Statements on Technical Documents, November 1 2017
DoD Directive 7045.14, "The Planning, Programming, Budgeting, and Execution (PPBE) Process," August 29, 2017
DoD Instruction 3305.13, "DoD Security Training," April 27 2018
DoD Instruction 5030.59, National Geospatial-Intelligence Agency (NGA) LIMITED DISTRIBUTION, Geospatial Intelligence, December 7, 2006
DoD Instruction 5200.1, "DoD Information Security Program and Protection of Sensitive Compartmented Information," May 1 2018
DoD Instruction 5210.83, DoD Unclassified Controlled Nuclear Information (DoD UCNI), February 22, 2018
DoD Instruction 7650.01, General Accounting Office (GAO) and Comptroller General Access to Records, May 15 2018
DoD Instruction 8523.01, Communications Security (COMSEC), April 22, 2008
DoD Manual 5105.21, Volume 1, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security," May 16, 2018
DoD Manual 5105.21, Volume 2, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," April 5 2018
DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," May 4 2018
DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," March 19 2013

DoD Manual 5200.01, Volume 3, “DoD Information Security Program: Protection of Classified Information,” March 19 2013
DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information (CUI),” May 9 2018
DoD Manual 5200.02, "Procedures For The DoD Personnel Security Program (PSP), April 3, 2017
Executive Order 12333, “United States Intelligence Activities,” December 4, 1981
Executive Order 13526, “Classified National Security Information,” December 29, 2009
Executive Order 13556, “Controlled Unclassified Information,” November 4, 2010
Federal Specification AA-C-2786, “Cabinet, Security, Information Processing System Storage”, April 7, 2007, as amended
Federal Specification AA-D-600, “Door, Vault, Security,”
Federal Specification AA-F-358J, “Filing Cabinet, Legal and Letter Size, Uninsulated, Security,” October 24, 2014, as amended
Federal Specification FF-L-2740B, “Locks, Combination, Electromechanical,” May 2, 2012, as amended
Federal Standard 832, “Federal Standard Construction Methods and Materials for Vaults,” September 1, 2002
Intelligence Community Directive 503, “Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation,” July 21 2015
Intelligence Community Directive 700, “Protection of National Intelligence,” June 7, 2012
Intelligence Community Directive 704, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information,” June 20 2018
Intelligence Community Directive 705, Sensitive Compartmented Information Facilities,
Intelligence Community Directive 710, “Classification and Control Markings System,” June 21 2013
Intelligence Community Technical Specifications (ICS) for Construction and Management of Sensitive Compartmented Information Facilities 705, September 28 2017
MQ-1/MQ-9, Predator, Security Classification Guide, May 1, 2006
National Disclosure Policy-1, “National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations” October 2, 2002
Office of the Chief of Naval Operations Instruction N9210.3, “Safeguarding of Naval Nuclear Propulsion Information,” June 7, 2010
Office of the Secretary of Defense Memorandum, “Request for Contractor Access to Planning, Programming, Budgeting, and Execution (PPBE) Documents and Data,” February 14,
Presidential Policy Directive-19, “Protecting Whistleblowers with Access to Classified Information,” October 10, 2012
SAE AMS-STD 595, “Colors Used in Government Procurement,” February 14, 2017
United States Code, Title 5
United States Security Authority for NATO Affairs Instruction 1-07, “Implementation of NATO Security Requirements,” April 5, 2007