Department of Defense

MANUAL

NUMBER 5200.01, Volume 4
February 24, 2012

USD(I)

SUBJECT: DoD Information Security Program: Controlled Unclassified Information (CUI)

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of CUI and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program. This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526 and E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume provides guidance for the identification and protection of CUI.

2. APPLICABILITY. This Volume:

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

b. Does not alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community pursuant to policies issued by the DNI.

c. Does NOT implement the new CUI program established by Reference (e). This Volume implements current DoD CUI policy according to Reference (b). The CUI program required by

Reference (e) will be implemented by a change to this Volume after the Federal policy is finalized.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy, in accordance with Reference (b), to:

a. Identify and protect national security information and CUI in accordance with national level policy issuances.

b. Promote information sharing, facilitate judicious use of resources, and simplify management through implementation of uniform and standardized processes.

c. Protect CUI from unauthorized disclosure by appropriately marking, safeguarding, disseminating, and destroying such information.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Volume is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE. This Volume is effective upon its publication to the DoD Issuances Website.

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. Identification and Protection of CUI
4. CUI Education and Training

Glossary

TABLE OF CONTENTS

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(b) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008
(c) DoD 5200.1-R, "Information Security Program," January 14, 1997 (cancelled by Volume 1 of this Manual)
(d) Executive Order 13526, "Classified National Security Information," December 29, 2009
(e) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
(f) Part 2001 of title 32, Code of Federal Regulations
(g) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
(h) Sections 552[1] and 552a[2] of title 5, United States Code
(i) Clause 252.204-7000 of the Defense Federal Acquisition Regulation Supplement
(j) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(k) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 7, 1998, with attached "Web Site Administration Policies and Procedures," November 25, 1998
(l) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
(m) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(n) DoD 5200.2-R, "Personnel Security Program," January 1, 1987
(o) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
(p) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
(q) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
(r) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(s) DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony by DoD Personnel as Witnesses," July 23, 1985
(t) DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
(u) DoD Instruction 7650.01, "Government Accountability Office (GAO) and Comptroller General Requests for Access to Records," January 27, 2009
(v) Chapters 22[3] and 33 of title 44, United States Code
(w) DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)," November 15, 1991
(x) DoD Instruction 5030.59, "National Geospatial-Intelligence Agency (NGA) LIMITED DISTRIBUTION Geospatial Intelligence," December 7, 2006
(y) Section 455 of title 10, United States Code

[1] Section 552 is also known as "The Freedom of Information Act"
[2] Section 552a is also known as "The Privacy Act of 1974, as amended"
[3] Chapter 22 is also known as "The Presidential Records Act of 1978"

(z) Department of Defense and United Kingdom Ministry of Defence, "Security Implementing Arrangement," January 27, 2003[4]
(aa) DoD Directive 3200.12, "DoD Scientific and Technical Information (STI) Program (STIP)," February 11, 1998
(ab) DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004
(ac) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," January 8, 2009
(ad) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(ae) Section 403 of title 50, United State Code, as amended
(af) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

[4] Available from OUSD(P), International Security Programs Directorate.

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall:

a. Direct, administer, and oversee the DoD Information Security Program for the Department of Defense.

b. Develop and issue guidance as required for the implementation of Reference (e) and its implementing directives.

c. As required by Reference (e), submit to the National Archives and Records Administration, in its role as CUI Executive Agent, a catalogue of proposed categories and subcategories of CUI, with proposed associated markings, and a plan for compliance with the requirements of Reference (e).

d. Establish requirements for collecting and reporting data as necessary to support fulfilling the requirements of Reference (e) and other national level policy issuances.

2. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) shall, in accordance with DoDD 5111.1 (Reference (g)), establish policies and procedures for disclosing DoD CUI to foreign governments and international organizations.

3. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components, in addition to the responsibilities in Volume 1 of this Manual, shall:

a. Identify, program for, and commit necessary resources to effectively implement the requirements for the protection of CUI as part of the Component's information security program.

b. Ensure that Component personnel are provided CUI education and training in accordance with Enclosure 4 of this Volume.

4. SENIOR AGENCY OFFICIALS. The senior agency officials, under the authority, direction and control of the Heads of the DoD Components, appointed in accordance with Enclosure 2 of Volume 1 of this Manual shall, in addition to the responsibilities in Volume 1:

a. Direct the head of each activity within the DoD Component that creates, handles, or stores CUI to appoint, in writing, an official to manage and oversee the CUI portion of the activity's information security program. If the activity also creates, handles, or stores classified information, the security manager appointed pursuant to paragraph 7.c of Enclosure 2 of Volume 1 may also be assigned this responsibility. Persons appointed to these positions shall be provided:

(1) The necessary authority to ensure personnel adhere to CUI requirements.

(2) Direct access to activity leadership.

(3) Organizational alignment that will ensure prompt and appropriate attention to CUI requirements.

(4) The training required by Enclosure 4.

b. Establish procedures to prevent unauthorized persons from accessing CUI.

c. Promptly address unauthorized disclosure of CUI, improper designation of CUI, and violations of the provisions of this Volume.

d. Direct, administer, and oversee an ongoing oversight program to evaluate and assess the effectiveness and efficiency of the DoD Component's implementation of that portion of the information security program pertaining to CUI.

(1) Evaluation criteria shall consider, at a minimum, CUI designation, safeguarding, education and training, and management and oversight.

(2) The oversight program shall include periodic review and assessment of the DoD Component's CUI information to ensure that such information is being properly marked and handled.

(3) DoD Component CUI education and training should be evaluated during oversight activities.

e. Direct, administer, and oversee CUI education and training as required by Enclosure 4, and ensure that DoD Component personnel receive education and training appropriate to their assigned duties.

ENCLOSURE 3

IDENTIFICATION AND PROTECTION OF CUI

1. GENERAL. In addition to classified information, certain types of unclassified information also require application of access and distribution controls and protective measures for a variety of reasons. In accordance with Reference (e), such information is referred to collectively as CUI. This enclosure identifies the controls and protective measures developed for DoD CUI (i.e., For Official Use Only (FOUO), Law Enforcement Sensitive (LES), DoD Unclassified Controlled Nuclear Information (DoD UCNI), and LIMITED DISTRIBUTION) as well as some of those developed by other Executive Branch agencies. This enclosure also addresses handling of certain foreign government information and the use of distribution statements on unclassified technical documents as a means to facilitate control, distribution, and release of such documents.

a. In accordance with Reference (b), information may not be designated CUI to:

(1) Conceal violations of law, inefficiency, or administrative error;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition; or

(4) Prevent or delay the release of information that does not require protection under statute or regulation.

b. Information shall not be designated CUI:

(1) To prevent or avoid its proper classification in accordance with the requirements of Reference (d) and Volume 1 of this Manual; or

(2) If there is significant doubt concerning the need for such designation in accordance with section 3.b of Reference (e).

c. Information that has been disclosed to the public under proper authority may not be subsequently designated or redesignated CUI.

d. The originator of a document is responsible for determining at origination whether the information may qualify 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; functional experts) from modifying the marking(s) applied or originally applying additional markings. In such cases, the originator shall be notified of the changes. Additionally, Freedom of Information Act Officers (individuals expert in section 552 of title 5, United States Code (U.S.C.) (also known as "The Freedom of Information Act" and hereinafter referred to as "FOIA" (Reference (h))) can be consulted for advice or training on the proper application of FOIA exemptions.

e. When CUI is to be provided to or generated by DoD contractors, the controls and protective measures to be applied shall be described in the pertinent contract documents (e.g., contract clause; statement of work; or DD Form 254, "Department of Defense Contract Security Classification Specification"). Solicitations and contracts shall use a non-disclosure of information clause that prohibits release of unclassified information to the public without approval of the contracting activity (e.g., clause 252.204-7000 of the Defense Federal Acquisition Regulation Supplement (Reference (i))). The clause shall also be made applicable to subcontractors.

f. ALL DoD unclassified information MUST BE REVIEWED AND APPROVED FOR RELEASE through standard DoD Component processes before it is provided to the public (including via posting to publicly accessible websites) in accordance with DoDD 5230.09 (Reference (j)), Deputy Secretary of Defense Memorandum (Reference (k)), and other applicable regulations. Unclassified information previously approved for release to the public may be shared with any foreign government or organization.

g. Release or disclosure of CUI to foreign governments or international organizations shall be in accordance with DoDD 5230.20 (Reference (l)) and other policy and procedures that may be established by the USD(P).

h. Some CUI is export-controlled information which may additionally be protected by law, Executive order, regulation, or contract. DoD officials must pay particular attention to export control regulations and to access restrictions on each type of CUI to ensure compliance with export requirements, especially when non-U.S. citizens are assigned to or visit their organizations.

i. Release or disclosure of CUI to non-U.S. citizens employed by the Department of Defense is permitted, provided access is within the scope of their assigned duties; access would further the execution of a lawful and authorized DoD mission or purpose and would not be detrimental to the interests of the Department of Defense or the U.S. Government; there are no contract restrictions prohibiting access; and the access complies with the requirements of DoDD 8500.01E (Reference (m)), DoD 5200.2-R (Reference (n)), and export control regulations, as applicable. In such cases, the non-U.S. citizen shall execute a nondisclosure agreement approved by appropriate DoD Component authorities.

j. CUI may be identified in security classification guides to ensure the information receives appropriate protection. If the security classification guide is subsequently cancelled, a separate memorandum or other guidance document may be issued to identify the declassified information, if any, that qualifies as CUI as well as any CUI previously cited in the guide.

k. For unauthorized disclosures of CUI, no formal security inquiry or investigation is required. However, appropriate management action shall be taken to fix responsibility for unauthorized disclosure of CUI whenever feasible or required by other guidance, and appropriate disciplinary action shall be taken against those responsible (see section 17 of Enclosure 3 of Volume 1 for sanctions). Unauthorized disclosure of some CUI (e.g., information protected by section 552a of Reference (h) (also known and hereinafter referred to as "The Privacy Act of

1974, as amended") or export-controlled technical data) may also result in civil and criminal sanctions against responsible persons. The DoD Component that originated the CUI shall be informed of its unauthorized disclosure.

l. Controlled unclassified documents and material that constitute permanently valuable records of the Government shall be maintained and disposed of according to DoDD 5015.2 (Reference (o)). Other controlled unclassified material shall be destroyed as specified in this Volume.

m. Exceptions to the guidance provided in this Volume must be approved by the USD(I). Requests shall be sent to the Deputy Under Secretary of Defense for Intelligence and Security through command channels.

2. FOUO INFORMATION

a. Description. FOUO is a dissemination control applied by the Department of Defense 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 of FOIA Exemptions 2 through 9. The FOIA specifies nine exemptions:

(1) Exemption 1. Information that is currently and properly classified.

(2) Exemption 2. Information that pertains solely to the internal rules and practices of the agency that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission.

(3) Exemption 3. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

(4) Exemption 4. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the Government's ability to obtain like information in the future, or impair the Government's interest in compliance with program effectiveness.

(5) Exemption 5. Inter- or intra-agency memorandums or letters containing information considered privileged in civil litigation. The most common privilege is the deliberative process privilege, which concerns documents that are part of the decision-making process and contain subjective evaluations, opinions, and recommendations. Other common privileges are the attorney-client and attorney work product privileges.

(6) Exemption 6. Information, the release of which would reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

(7) Exemption 7. Records or information compiled for law enforcement purposes that:

(a) Could reasonably be expected to interfere with law enforcement proceedings.

(b) Would deprive a person of a right to a fair trial or impartial adjudication.

(c) Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others.

(d) Disclose the identity of a confidential source.

(e) Disclose investigative techniques and procedures.

(f) Could reasonably be expected to endanger the life or physical safety of any individual.

(8) Exemption 8. Certain records of agencies responsible for supervision of financial institutions.

(9) Exemption 9. Geological and geophysical information (including maps) concerning wells.

b. Application

(1) It is the responsibility of the document's originator to determine at origination whether the information may qualify for FOUO status and to ensure markings are applied as required. Further details on the types of information that may qualify for the specified exemptions and FOUO status can be found in Chapter 3 of DoD 5400.7-R (Reference (p)).

(2) Information that is currently and properly classified shall be withheld from mandatory release in accordance with FOIA Exemption 1. The marking "FOR OFFICIAL USE ONLY" is applied to information that can reasonably be expected to qualify for exemption under one or more of FOIA Exemptions 2 through 9. By definition, information must be unclassified in order to be designated FOUO. This means that:

(a) Information cannot be marked as classified and FOUO at the same time, because no individual element of information can be simultaneously classified and FOUO. Therefore, classified documents containing FOUO information cannot bear an overall document marking of FOUO. However, portions or pages of a classified document that contain only FOUO information will be marked in a manner that identifies the FOUO content.

(b) Information that is declassified may be designated and marked as FOUO only 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 of FOIA Exemptions 2 through 9.

(c) FOUO is not authorized as a means of protecting information that otherwise does not merit protection as classified for national security reasons.

c. Markings

(1) Information that has been determined to qualify for FOUO status shall 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) Marking information FOUO does not automatically qualify it for exemption from public release pursuant to the FOIA. If a request for a record is received, the information shall be reviewed in accordance with the procedures of Reference (p) to determine if it truly qualifies for exemption. Similarly, the absence of the FOUO marking does not automatically mean the information shall be released. Some types of records (e.g., personnel records) are not normally marked FOUO, but may still qualify for withholding in accordance with the FOIA. Information marked FOUO shall not specify, or have annotated, a FOIA exemption number.

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

(a) Each document determined to contain FOUO information shall identify the originating agency or office. This information shall 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 shall 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 shall 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 shall be marked at both the top and bottom.

(d) Subjects, titles, and each section, part, paragraph, or similar portion of an FOUO document shall 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 e-mail, containing FOUO information shall be marked as required by paragraph 2.c of this enclosure. Unclassified messages containing FOUO information shall be marked "FOR OFFICIAL USE ONLY" (optionally "UNCLASSIFIED//FOR OFFICIAL USE ONLY" or "UNCLASSIFIED//FOUO")

before the beginning of the text and shall 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, shall be marked with the following statement or a similar one: "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, chart, maps, films, sound recordings), the requirement remains to identify, as clearly as possible, the information that requires protection. The main concern is that holders and users of the material are clearly notified of the presence of FOUO information. The markings required by this enclosure shall be applied either on the item or the documentation that accompanies it. Particular requirements and exceptions are noted in the following subparagraphs.

1. Information Technology and Other Electronic Media. Conspicuously mark removable storage media used with computers, information technology systems, and other electronic devices and any other device on which data is stored and which normally is removable from the system by the user or operator. (Examples of such media include, but are not limited to, compact discs (CDs), digital video discs (DVDs), 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, tape cassettes, and micro-cassettes.) Internal media identification will include FOUO markings in a form suitable for the media. Where size permits, all such devices bearing FOUO information must be conspicuously marked on the device or a label affixed thereto. Where size or technology preclude marking or affixing a label to the removable device itself (e.g., compact disc-read only memory (CD-ROM), memory chips), the label may be affixed to the container in which the device is stored.

2. Blueprints, Engineering Drawings, Charts, and Maps. Mark blueprints, engineering drawings, charts, maps, and similar items not contained within another document, with the FOUO designation when applicable. The marking shall be unabbreviated, conspicuous, and applied top and bottom, if possible, in such a manner as to ensure reproduction on any copies. The legend or title shall also be marked. The parenthetical marking "(FOUO)" or "(U//FOUO)" following the legend or title may be used. If the blueprints, maps, and other items are large enough that they are likely to be rolled or folded, additional FOUO markings shall be placed to be visible when the item is rolled or folded.

3. Photographic Media

a. Mark photographs and negatives "FOR OFFICIAL USE ONLY" (optionally "UNCLASSIFIED//FOR OFFICIAL USE ONLY" or "UNCLASSIFIED//FOUO"). Mark photographs on the face, if possible. Where this cannot be done, the marking may be placed on the reverse side. Digital photographs may be edited to place the markings on the face of the photograph.

b. Mark roll negatives and positives, and other film containing FOUO either on the film itself or on the canister, if one is used. If placed on the film itself, the marking shall be placed at the beginning and end of the roll.

c. Mark slides and transparencies on the image area of the item and also on the border, holder, or frame, if any. Information on the image area of each slide or transparency shall be portion marked in accordance with subparagraph 2.c.(3)(d) of this enclosure.

d. Mark DVDs, video tapes, and motion picture films at the beginning and end of the presentation (i.e., the played or projected portion). Discs, reels, and cassettes shall be marked and, when stored in a container, the container shall also be marked.

4. Sound Recordings. Place an audible statement of the designation of FOUO at the beginning and end of sound recordings. Reels or cassettes shall be marked as required, and when stored in a container, the container shall be marked.

5. Microfilm, Microfiche, and Similar Microform Media. Mark microfilm, microfiche, and similar microform media "FOR OFFICIAL USE ONLY" (optionally "UNCLASSIFIED//FOR OFFICIAL USE ONLY" or "UNCLASSIFIED//FOUO") in the image area that can be read or copied. Such media also shall have this marking applied so it is visible to the unaided eye. Any containers shall contain the required markings, except no markings are required if the container is transparent and the marking on the media itself is clearly visible.

(4) Classified documents and material, including those in electronic form, that also contain FOUO information shall be marked in accordance with Volume 2 of this Manual, with FOUO information identified as follows:

(a) Overall markings on the document shall follow the guidance in Volume 2 of this Manual. No additional special markings are required on the face of the document because it contains FOUO information.

(b) Pages of the document that contain classified information shall be marked in accordance with Volume 2 of this Manual. Pages that contain FOUO information but no classified information shall be marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" or "UNCLASSIFIED//FOUO" at the top and bottom if the overall document classification is not used as the page marking.

(c) Portions of the document shall be marked with their classification in accordance with Volume 2 of this Manual. If there are unclassified portions that contain FOUO information, use the parenthetical notation "(U//FOUO)" at the beginning of the portion. If a portion of a classified document contains both classified and FOUO information, the appropriate classification designation is sufficient to protect the information, and no additional marking shall be used to designate the FOUO content.

(d) Each portion of electronically transmitted classified messages, including e-mail, containing FOUO information shall be marked appropriately.

(5) FOUO information disseminated outside the Department of Defense shall also bear a marking on the outside of the front cover, first page, or at the beginning of the text that states that the information may be exempt from mandatory disclosure in accordance with the FOIA. A statement similar to that shown in Figure 1 is sufficient. A FOIA exemption number shall NOT be applied.

Figure 1. Exemption Notice for FOUO Disseminated Outside of the Department of Defense

This document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.

(6) Technical documents that require a distribution statement restricting disclosure and/or an export control warning notice pursuant to DoDD 5230.24 (Reference (q)) and section 8 of this enclosure should be marked as FOUO when appropriate, in addition to the required distribution statement.

d. 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, not with the prospective recipient.

(3) Information designated as FOUO may be disseminated within the DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense, provided that dissemination is consistent with any further controls imposed by a distribution statement. (See section 8 of this enclosure for information on distribution statements.)

(4) Information designated as FOUO may be disseminated to representatives of foreign governments and international organizations to the extent that disclosure would further the execution of a lawful and authorized mission or purpose. Such dissemination shall be in compliance with Reference (l) and other applicable statutes, regulations, and policies. (See paragraphs 1.g and 1.h of this enclosure for general disclosure guidance.)

(5) DoD holders of information designated as FOUO are authorized to disseminate such information to officials in other departments and agencies of the Executive and Judicial Branches to fulfill a Government function provided such dissemination is consistent with any further controls imposed by distribution statements or other regulations. If the information is covered by

the Privacy Act of 1974, as amended, disclosure is authorized only if the requirements of DoD 5400.11-R (Reference (r)) are also satisfied. Records thus transmitted shall be marked as required by paragraph 2.c of this enclosure, and the recipient shall be advised that the information may qualify for exemption from public disclosure, pursuant to the FOIA, and that special handling instructions do or do not apply. Release of official information in litigation and testimony by DoD personnel as witnesses shall be in accordance with DoDD 5405.2 (Reference (s)).

(6) Release of FOUO information to Congress shall be in accordance with DoDI 5400.04 (Reference (t)). If the information is covered by the Privacy Act of 1974, as amended, disclosure is authorized only if the requirements of Reference (r) are also satisfied.

(7) DoDI 7650.01 (Reference (u)) governs release of FOUO information to the Government Accountability Office (GAO). If the information is covered by the Privacy Act of 1974, as amended, disclosure is authorized only if the requirements of Reference (r) are also satisfied.

(8) Records released outside of the Department of Defense, including to the Congress or GAO, should be reviewed to determine whether the information warrants FOUO status. If it does not, any prior FOUO markings shall be removed by lining-through or other appropriate means. If withholding criteria are met, the records shall be marked FOUO and the recipient provided an explanation for the marking.

(9) FOUO information may be shared with State, local, or tribal government officials, provided a specific need to know has been established and the information is shared in furtherance of an official governmental purpose. In all cases, the recipient must agree to the stipulation that the information shall be withheld by the recipient from public release. Records thus shared shall be marked in accordance with paragraph 2.c of this enclosure, and the recipient shall be advised whether special handling instructions do or do not apply.

e. Protection of FOUO Information

(1) During working hours, reasonable steps shall 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). 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 shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc.

(2) FOUO information and material 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, website, or e-mail) shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI) or transport layer security (e.g., https). Use of wireless telephones should be avoided when other options are available. Transmission of FOUO by facsimile machine (fax) is permitted; 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).

(3) FOUO information may only be posted to DoD websites consistent with security and access requirements specified in Reference (k).

(4) Additional guidance regarding FOUO information that may also require protection pursuant to the Privacy Act of 1974, as amended, may be found in Reference (r).

(5) Record copies of FOUO documents shall be disposed of according to provisions of chapter 33 of title 44, U.S.C. (Reference (v)) and the DoD Component records management directives. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information.

(6) The originator or other competent authority (e.g., initial FOIA denial and appellate authorities) shall terminate the FOUO status of specific information when circumstances indicate that the information no longer requires protection from public disclosure. When the FOUO status of information is terminated in this manner, all known holders shall be notified, to the extent practical. Upon notification, holders shall efface or remove the FOUO markings, but records in file or storage need not be retrieved solely for that purpose. Information whose FOUO status has been terminated shall not be released to the public without the review and approval required by paragraph 1.f of this enclosure.

3. LES INFORMATION

a. Description. "Law Enforcement Sensitive" is a marking sometimes applied, in addition to the marking "FOR OFFICIAL USE ONLY," by the Department of Justice and other activities in the law enforcement community, including those within the Department of Defense. It denotes that the information was compiled for law enforcement purposes and should be afforded security in order to protect certain legitimate Government interests, including the protection of:

(1) Enforcement proceedings.

(2) The right of a person to a fair trial or an impartial adjudication; grand jury information.

(3) Personal privacy, including records about individuals requiring protection in accordance with the Privacy Act of 1974, as amended.

(4) The identity of a confidential source, including a State, local, or foreign agency or authority or any private institution that furnished information on a confidential basis.

(5) Information furnished by a confidential source.

(6) Proprietary information.

(7) Techniques and procedures for law enforcement investigations or prosecutions; guidelines for law enforcement investigations when disclosure of such guidelines could reasonably be expected to risk circumvention of the law, or jeopardize the life or physical safety of any individual, including the lives and safety of law enforcement personnel.

b. Markings

(1) In unclassified documents containing LES information, the phrase "Law Enforcement Sensitive" shall accompany the phrase "FOR OFFICIAL USE ONLY" at the bottom of the outside of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one). Each page containing FOUO-LES information shall be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" at the bottom.

(2) Classified documents containing such information shall be marked in accordance with Volume 2 of this Manual, except that pages containing LES information but no classified information shall be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" on the top and bottom. Use separate portions for LES information; do not commingle LES information with classified information in the same portion.

(3) Portions of DoD unclassified documents that contain FOUO-LES information shall be marked with the parenthetical notation "(FOUO-LES)" at the beginning of the portion. If an unclassified portion of a classified document contains FOUO-LES information, the portion marking (U//FOUO-LES) shall be used. If a portion of a classified document contains both classified and FOUO-LES information, the appropriate classification designation is sufficient to protect the information and no additional marking shall be used to designate the LES content.

(4) Documents containing LES information shall be marked on the first page with the warning statement shown in Figure 2.

Figure 2. LES Warning Statement

LAW ENFORCEMENT SENSITIVE: The information in this document marked FOUO-LES is the property of (insert organization) and may be distributed within the Federal Government (and its contractors) to law enforcement, public safety and protection, and intelligence officials and individuals with a need to know. Distribution to other entities without prior (insert organization) authorization is prohibited. Precautions shall be taken to ensure this information is stored and destroyed in a manner that precludes unauthorized access. Information bearing the FOUO-LES marking may not be used in legal proceedings without prior authorization from the originator. Recipients are prohibited from posting information marked FOUO-LES on a website or unclassified network.

c. Access. The criteria for allowing access to FOUO-LES information are the same as those used for FOUO information.

d. Protection. Within the Department of Defense, FOUO-LES information shall be safeguarded and destroyed as required for FOUO information.

4. DoD UCNI

a. Description. DoD UCNI is unclassified information on 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 DoDD 5210.83 (Reference (w)) only when it is determined that 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.

b. Application. Information may be designated DoD UCNI by the Heads of the DoD Components and individuals delegated authority in accordance with Reference (w).

c. Markings

(1) Unclassified documents and material, including those in electronic form, containing DoD UCNI shall be marked as follows:

(a) Documents shall be marked with the phrase "DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" (or alternately "DOD UCNI") at the bottom on the outside of the front cover, if any; the outside of the back cover, if any; the first page; and each individual page containing DoD UCNI.

(b) Portions of the document that contain DoD UCNI shall be marked with the parenthetical notation "(DCNI)" at the beginning of the portion.

(2) Classified documents and material containing DoD UCNI shall be marked in accordance with Volume 2 of this Manual.

(a) Pages with no classified information but containing DoD UCNI shall be marked "UNCLASSIFIED//DOD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" or "UNCLASSIFIED//DOD UCNI" at the top and bottom, unless the page is marked with the overall classification of the document.

(b) Portions of the document that contain DoD UCNI, but no classified information, shall be marked with the parenthetical notation "(U//DCNI)" at the beginning of the portion.

Portions containing both DoD UCNI and classified information shall be marked "DCNI" in addition to the required classification marking (e.g., "(S//DCNI)").

(3) Material in other formats (e.g., slides, computer media, films) shall bear conspicuous markings that alert the holder or viewer that the material contains DoD UCNI. See subparagraph 2.c.(3)(g) of this enclosure for guidance on marking such material.

(4) Transmittal documents shall call attention to the presence of DoD UCNI attachments by using a statement in the text or marking at the bottom of the transmittal document. A statement such as "The attached document contains DoD Unclassified Controlled Nuclear Information (DoD UCNI)" is sufficient.

(5) Documents and material containing DoD UCNI and transmitted outside the Department of Defense shall bear an expanded marking on the face of the document so that non-DoD holders understand that DoD UCNI is exempt from mandatory public disclosure under the FOIA. A statement similar to the one shown in Figure 3 shall be used:

Figure 3. DoD UCNI Statement on Information Transmitted Outside of the Department of Defense

Department of Defense
Unclassified Controlled Nuclear Information
Exempt from mandatory disclosure under
5 U.S.C. 552(b)(3), as authorized by 10 U.S.C. 128
Unauthorized dissemination subject to civil and criminal sanctions
under Section 148 of the Atomic Energy Act of 1954, as amended
(42 U.S.C. 2168).

d. Access. Access to DoD UCNI shall be granted only to persons who have a valid need to know the information and are specifically eligible for access in accordance with the provisions of Reference (w).

(1) Recipients shall be made aware of the status of such information, and transmission shall be by means that preclude unauthorized disclosure or dissemination.

(2) DoD holders of DoD UCNI are authorized to convey such information to officials in other U.S. departments or agencies on a need-to-know basis to fulfill a Government function.

e. Protection

(1) When not commingled with classified information, DoD UCNI may be sent by first-class mail in a single, opaque envelope or wrapping.

(2) Except in emergencies, transmission of DoD UCNI, to include voice, facsimile, and e-mail, shall be via approved secure communications circuits and equipment only.

(3) During working hours, reasonable measures shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving DoD UCNI unattended where unauthorized personnel are present). After working hours, DoD UCNI 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, DoD UCNI shall be stored in locked buildings, rooms, desks, file cabinets, bookcases, or similar items.

(4) Record copies of DoD UCNI documents shall be disposed of in accordance with chapter 33 of Reference (v) and the DoD Component records management directives. Non-record DoD UCNI documents may be destroyed by shredding or burning or by any of the means approved for the destruction of classified information.

(5) DoD UCNI is exempt from mandatory public disclosure under Exemption 3 of the FOIA.

5. LIMITED DISTRIBUTION INFORMATION

a. Description. "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 (Reference (x)) contains details of policies and procedures regarding use of the LIMITED DISTRIBUTION caveat. These policies and procedures are summarized in this section and in Enclosure 4 of Volume 2 of this Manual.

b. Application

(1) Information that qualifies for withholding from public release pursuant to section 455 of title 10, U.S.C. (Reference (y)) may be designated as LIMITED DISTRIBUTION in accordance with Reference (x).

(2) The marking indicates distribution of certain unclassified geospatial intelligence is limited to the Department of Defense and authorized DoD contractors. Other dissemination requests or requirements shall be referred to NGA for approval.

c. Marking. Information or material designated as LIMITED DISTRIBUTION, or derived from such information or material, shall, unless otherwise approved by the Director, NGA, be marked "LIMITED DISTRIBUTION" and shall carry the notice shown in Figure 4 on the front page. Portions of the document that contain LIMITED DISTRIBUTION information shall be marked at the beginning of the portion with the parenthetical notation "(DS)" for an unclassified document or "(U//DS)" for a classified document.

Figure 4. LIMITED DISTRIBUTION Notice

Distribution authorized to DoD, IAW 10 U.S.C. 130 & 455.
Release authorized to U.S. DoD contractors IAW
48 C.F.R. 252.245-7000.
Refer other requests to
Headquarters, NGA, ATTN: Release Officer, Mail Stop S82-OIAD,
7500 Geoint Drive, Springfield, VA 22150-7500
Destroy IAW DoD Manual 5200.01.
Removal of this caveat is prohibited.

d. Access

(1) Information bearing the LIMITED DISTRIBUTION caveat shall be disseminated by NGA to Military Departments or other DoD Components, to DoD contractors, and to authorized grantees for the conduct of official DoD business.

(2) DoD civilian, military, and contractor personnel of a recipient Military Department, other DoD Component, contractor, or grantee may be granted access to information bearing the LIMITED DISTRIBUTION caveat provided they have been determined to have a valid need to know such information in connection with the accomplishment of official business for the Department of Defense. Recipients shall be made aware of the status of such information, and transmission shall be by means to preclude unauthorized disclosure or release. Further dissemination of information bearing the LIMITED DISTRIBUTION caveat by receiving contractors or grantees to another Military Department, other DoD Component, contractor, or grantee, or dissemination by any recipient Military Service, DoD Component, contractor, or grantee to any person, agency, or activity outside the Department of Defense, requires the express written approval of the Director, NGA.

(3) Information bearing the LIMITED DISTRIBUTION caveat, or information derived therefrom, shall not be released, made accessible, or sold to foreign governments or international organizations, without the express written approval of the Director, NGA. This requirement includes Foreign Security Assistance transactions or arrangements, transfer or loan of any weapon or weapon system that uses such information, intended use in mission planning systems, and/or sale through the Foreign Military Sales process.

(4) All FOIA requests for information bearing the LIMITED DISTRIBUTION caveat, or derived therefrom, shall be referred to NGA consistent with Reference (x).

e. Protection

(1) LIMITED DISTRIBUTION information shall be stored in the same manner approved for FOUO information.

(2) Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be stored on systems accessible by contractors or other individuals who are not directly working on a DoD contract and who do not require such access in the conduct of official DoD business.

(3) Transmission of LIMITED DISTRIBUTION information and materials shall be by means that preclude unauthorized disclosure or release. LIMITED DISTRIBUTION information cannot be processed on or transmitted via unencrypted or unsecured systems accessible by the public. Electronic transmission of such information (e.g., voice, data, or facsimile) shall be by approved secure communications systems or systems utilizing protective measures such as PKI.

(4) LIMITED DISTRIBUTION information, or derivative information, may be posted to DoD websites only in accordance with security and access requirements specified in Reference (k). Publicly-accessible websites shall not contain LIMITED DISTRIBUTION information.

(5) When no longer required, all LIMITED DISTRIBUTION information and copies shall be returned to NGA or destroyed in a manner sufficient to prevent its reconstruction.

6. OTHER AUTHORIZED DESIGNATIONS

a. Department of State (DoS) Sensitive But Unclassified (SBU) Information

(1) Description. 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.

(2) Markings

(a) Unclassified documents containing DoS SBU information shall be marked "SENSITIVE BUT UNCLASSIFIED" at the bottom of the outside of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one). Each page containing DoS SBU information shall be marked "SENSITIVE BUT UNCLASSIFIED" at the bottom. Portions of the document that contain DoS SBU shall be marked with the parenthetical notation "(SBU)" at the beginning of the portion.

(b) When DoS information carries the additional dissemination restriction NOFORN (i.e., the document is marked "SBU NOFORN" or "SENSITIVE BUT UNCLASSIFIED NOFORN"), the NOFORN restriction shall be carried forward in the markings at the bottom of the cover pages, the title page, and each internal page and in the portion marking of portions containing such information. Portions of the document that contain information not releasable to foreign nationals (i.e., NOFORN information) shall be marked with the parenthetical notation "(SBU-NF)" at the beginning of the portion.

(c) When a document contains both DoS SBU and FOUO portions, the SBU markings supersede FOUO in the markings at the bottom of the cover and title pages and at the bottom of internal document pages.

(d) No requirement exists to re-mark existing material containing DoS SBU information.

(e) See Volume 2 of this Manual for guidance on marking classified documents containing DoS SBU information.

(3) Access. Within the Department of Defense, the criteria for allowing access to DoS SBU information are the same as those used for FOUO information, EXCEPT that information marked "SBU NOFORN" (or portion marked "(SBU-NF)") shall not be provided to any person who is not a U.S. citizen without the approval of the DoS activity that originated the information.

(4) Protection of DoS SBU Information. Within the Department of Defense, DoS SBU information shall be protected as required for FOUO information.

b. Drug Enforcement Administration (DEA) Sensitive Information

(1) Description. DEA Sensitive information is unclassified information that the DEA originates and that 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 have been authorized to designate information as DEA Sensitive; the Department of Defense agreed to implement protective measures for DEA Sensitive information in its possession. Types of information to be protected include:

(a) Information and material that is investigative in nature.

(b) Information and material to which access is restricted by law.

(c) Information and material that is critical to the operation and mission of the DEA.

(d) Information and material the disclosure of which would violate a privileged relationship.

(2) Markings

(a) Unclassified documents containing DEA Sensitive information shall be marked "DEA SENSITIVE" at the top and bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one). Each page containing DEA Sensitive information shall be marked "DEA SENSITIVE" top and bottom. Portions of unclassified DoD documents that contain DEA Sensitive information shall be marked with the parenthetical notation "(DSEN)" at the beginning of the portion.

(b) Classified documents containing DEA Sensitive information shall be marked in accordance with Volume 2 of this Manual. Pages containing DEA Sensitive information but no classified information may be marked "UNCLASSIFIED//DEA SENSITIVE" top and bottom. If a portion of a classified document contains DEA Sensitive information, include the "DSEN" marking after the parenthetical classification marking (e.g., (U//DSEN)). Classified and DEA Sensitive portions should be kept separate.

(3) Access. Access to DEA Sensitive information shall be granted only to persons who have a valid need to know the information. A security clearance is not required for access to unclassified DEA Sensitive information. DEA Sensitive information in the possession of the Department of Defense may not be released outside the Department without DEA authorization.

(4) Protection

(a) DEA Sensitive material may be transmitted within the continental United States (CONUS) by first class mail. Transmission outside CONUS shall be by a means approved for transmission of Secret material (see Enclosure 4 of Volume 3 for transmission guidance). Non-government package delivery and courier services may not be used. Enclose the material in two opaque envelopes or containers, the inner one marked "DEA SENSITIVE" on both sides.

(b) Electronic transmission of DEA Sensitive information within CONUS shall be over secure (i.e., encrypted) communications circuits whenever possible; electronic transmission outside CONUS must be over secure communications circuits.

(c) Reproduction of DEA Sensitive information and material shall be limited to that required for operational needs.

(d) DEA Sensitive material shall be destroyed by a means approved for destruction of material classified Confidential.

7. FOREIGN GOVERNMENT INFORMATION

a. In order to ensure the protection of foreign government information that is provided to a DoD Component marked "RESTRICTED" or on the condition that it will be treated "in confidence," such information shall be marked in accordance with Volume 2 of this Manual and handled in accordance with Enclosure 2 of Volume 3 of this Manual.

b. A revision to the U.S./United Kingdom (UK) Security Implementing Arrangement (Reference (z)) that deals with industrial operations specifies that DoD contactors operating under COMMERCIAL contracts with the UK are allowed to treat documents received from the UK bearing the marking "UK RESTRICTED" in a manner similar to FOUO. Pursuant to Reference (z), the UK must include its requirements for the marking and handling of "UK RESTRICTED" information in the applicable contract. The agreement does NOT apply to, nor permit, such handling of "UK RESTRICTED" information by DoD Components or by

contractors when performing on DoD contracts and the provisions of paragraph 7.a of this enclosure apply.

8. DISTRIBUTION STATEMENTS ON TECHNICAL DOCUMENTS

a. Description. Reference (q) requires distribution statements to be placed on classified and unclassified scientific and technical documents created under the DoD Scientific and Technical Information Program (see DoDD 3200.12 (Reference (aa))). These statements are intended to facilitate control, secondary distribution, and release of these documents without the need to repeatedly obtain approval or authorization from the controlling DoD office.

(1) Distribution statements are to be applied to all newly created technical documents generated by DoD-funded research, development, test, and evaluation programs and to newly created technical documents and other technical information (e.g., test plans, computer software) that can be used or adapted for use in development, manufacture, or operation of any military or space equipment or related technology. They are not intended for use on program documentation such as administrative documents, contracting documents, and general correspondence, etc., unless these documents also contain technical information.

(2) The wording of the distribution statements specified by Reference (q) may not be modified to specify additional distribution, such as distribution to foreign governments. However, where other markings are authorized and used in accordance with statute, regulation, or other policy (e.g., North Atlantic Treaty Organization markings, REL TO), those markings may be used to further inform distribution decisions.

b. Application. DoD Components generating or responsible for technical documents shall determine if one or more of the reasons for controlled dissemination as specified in Reference (q) apply and mark the documents appropriately before initial distribution. Refer to Reference (q) for details on use of the markings and allowable reasons for controlling distribution.

(1) Unclassified DoD technical documents shall bear one of the distribution statements specified in Reference (q) and shown in the Table. Documents recommended for public release (i.e., marked with Distribution Statement A) must also be reviewed in accordance with Reference (j).

(2) Classified technical documents shall be assigned Distribution Statements B, C, D, E, or F. The distribution statement assigned to a classified document shall be retained on the document after its declassification or until specifically changed or removed by the controlling DoD office. Technical documents that are declassified and have no distribution statement assigned shall be handled in accordance with Distribution Statement F until changed by the controlling DoD office.

(3) Documents containing export-controlled technical data shall be marked with the applicable export-control statement, as specified by paragraph E3.1.1.8 of Reference (q), and

assigned Distribution Statement B, C, D, E, F, or X. Export-controlled information may NOT be posted to publicly-accessible websites.

Table. Text of Distribution Statements

Distribution A	Approved for public release, distribution is unlimited.
Distribution B	Distribution authorized to U.S. Government Agencies only; (reason); (date). Other requests for this document shall be referred to (controlling DoD office)
Distribution C	Distribution authorized to U.S. Government agencies And their contractors; (reason); (date) Other requests for this document shall be referred to (controlling DoD office).
Distribution D	Distribution authorized to the DoD and U.S. DoD contractors only; (reason); (date). Other requests for this document shall be referred to (controlling DoD office).
Distribution E	Distribution authorized to DoD Components only; (reason); (date); Other requests for this document shall be referred to (controlling DoD office).
Distribution F	Further distribution only as directed by (controlling DoD office) or higher DoD authority; (date).
Distribution X	Distribution authorized to U. S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (controlling DoD office).

(4) The existence of a distribution statement on a document does not automatically qualify the document for, nor is it a basis for, exempting the document from release under the FOIA. A FOIA exemption must apply in order to preclude disclosure in accordance with the FOIA. Paragraph 2.a of this enclosure and Chapter 3 of Reference (p) provide additional information on FOIA exemptions. When appropriate, technical documents qualifying for FOIA exemptions should be marked as FOUO in addition to the required distribution statement.

(5) The distribution statement shall be displayed conspicuously so as to be recognized readily by recipients. For standard written or printed material, the distribution statement shall appear on the front page of the document (i.e., the first page or cover page). If the information is not prepared in the form of an ordinary document and does not have a cover or title page (such as forms and charts), the applicable distribution statement shall be stamped, printed, written, or affixed by other means in a conspicuous position.

(6) When possible, parts that contain information creating the requirement for a distribution statement shall be prepared as an appendix to permit broader distribution of the basic document.

ENCLOSURE 4

CUI EDUCATION AND TRAINING

1. REQUIREMENTS. The Heads of the DoD Components shall ensure that their personnel receive CUI education and training that:

a. Provides necessary knowledge and information to enable quality performance of CUI designation, marking, and protection functions.

b. Promotes understanding of the DoD Information Security Program policies and requirements and their importance to the national interests.

c. Instills and maintains continuing awareness of security requirements.

d. Assists in promoting a high degree of motivation to support program goals.

2. CUI EDUCATION AND TRAINING RESOURCES

a. CUI education and training may be accomplished by establishing programs within the DoD Component, using external resources such as the Defense Security Service Academy, or a combination of the two.

b. DoD Components may, if desired, combine into one overall program the education and training requirements of this enclosure and those for classified information specified in Volume 3 of this Manual.

3. INITIAL ORIENTATION. All personnel in the organization, including DoD civilians, military members and on-site support contractors, shall receive an initial orientation to the DoD Information Security Program.

a. This initial orientation is intended to:

(1) Define classified information and CUI and explain the importance of protecting such information.

(2) Produce a basic understanding of security policies and principles.

(3) Notify personnel of their responsibilities within the security program, and inform them of the administrative, civil, or criminal sanctions that can be applied when appropriate.

(4) Provide individuals enough information to ensure the proper protection of classified and controlled unclassified information in their possession, including actions to be taken if such

information is discovered unsecured, a security vulnerability is noted, or the individual believes a person has been seeking unauthorized access to such information.

(5) Inform personnel of the need for review of ALL unclassified DoD information prior to its release to the public.

b. Security educators shall also consider including in the initial orientation identification of the senior agency official and activity security management personnel, a description of their responsibilities, and whether they are involved in the protection of classified or controlled unclassified information. If not included in the initial orientation, such information must be included in the training required by paragraph 3.c. of this enclosure.

c. In addition to the requirements in paragraphs 3.a. and 3.b. of this enclosure, upon initial entry into a position that requires CUI access, all personnel shall receive training on CUI policies, principles, and practices, including:

(1) The responsibilities of agency personnel who create or handle CUI.

(2) The characteristics that qualify information for designation as CUI and the importance of properly applying CUI markings.

(3) The fact that CUI encompasses multiple different types of information and that each type may have differing marking and protection requirements.

(4) The major categories of CUI used within the Department of Defense.

(5) The marking and protection requirements for FOUO information and other categories of CUI routinely used by the organization.

(6) Where to find detailed guidance on marking, handling, storing, transmitting, sharing, and destroying the various types of CUI.

(7) What constitutes an unauthorized disclosure of CUI and the criminal, civil, and administrative sanctions that may be taken against an individual who fails to protect CUI.

(8) The steps an individual shall take when he or she believes CUI has not been, or is not being, properly protected.

(9) The use of information systems to create, process, store, or transmit CUI. Where appropriate, this training may be combined with the information assurance training required by DoDD 8570.01 (Reference (ab)). Marking requirements for information (e.g., documents, e-mail, briefings, databases, web-based information, spreadsheets) in electronic format and application of CUI requirements to electronic storage media should specifically be addressed.

(10) The requirement for DoD personnel, while acting in an official capacity, to have information prepared for public release approved in accordance with Reference (j) and DoDI

5230.29 (Reference (ac)) and, while acting in a private capacity and not in connection with their official duties, to have information prepared for public release through non-DoD forums or media reviewed for clearance if it meets the criteria in Reference (ac).

(11) The precautions that should be taken before attendance at professional meetings or conferences where foreign participation is likely and/or travel to foreign countries where special concerns about possible exploitation exist, when appropriate for the activity's mission or functions.

4. REQUIREMENTS FOR INFORMATION SECURITY PROGRAM PERSONNEL. Individuals with specified duties in the information security program shall be provided security education and training that is commensurate with job responsibilities and sufficient to permit effective performance of those duties. The education and training may be provided before or concurrent with assuming those duties.

5. ADDITIONAL TRAINING REQUIREMENTS. Additional CUI education and training may be required for personnel or organizations that:

a. Review and approve information for release to the public, including through the use of websites.

b. Are involved with acquisition programs subject to DoDD 5000.01 (Reference (ad)).

c. Are involved with international programs (see Glossary for definition).

d. Share CUI with State, local, tribal, and private sector officials and/or with foreign government representatives.

6. ANNUAL REFRESHER TRAINING. At a minimum, DoD civilians, military members, and on-site support contractors with access to CUI shall receive annual refresher training that reinforces the policies, principles, and procedures covered in their initial and specialized CUI training. Such training may be integrated with the annual security refresher required by section 7 of Enclosure 6 of Volume 3 or the annual information assurance awareness refresher, as required by Reference (ab), as appropriate. Refresher training shall also address the threat and the techniques foreign intelligence activities use while attempting to obtain DoD CUI and advise personnel of penalties for unauthorized disclosures. The importance of unclassified information, its potential sensitivity, and the requirement to have all information reviewed and approved for release prior to public disclosure or Web posting shall be reiterated. Refresher training shall also address relevant changes in CUI policy or procedures and issues or concerns identified during DoD Component oversight reviews.

7. CONTINUING CUI EDUCATION AND TRAINING. CUI education shall be a continuous process. Periodic briefings, training sessions, and other formal presentations shall be supplemented with other information and promotional efforts to ensure that continuous awareness and performance quality is maintained. The use of job performance aids and other substitutes for formal training is encouraged when they are determined to be the most effective means of achieving program goals. The circulation of directives or similar material on a "read-and-initial" basis shall not be considered as the sole means of fulfilling any of the specific requirements of this enclosure.

8. OUT-PROCESSING. The DoD Components shall establish procedures to ensure that employees with access to CUI who leave the organization are advised during their out-processing of:

a. Their continued responsibility to protect the CUI to which they have had access.

b. The process for reporting any unauthorized attempt to gain access to such information.

c. The prohibitions against retaining CUI material when leaving the organization.

d. The potential civil and criminal penalties for failure to fulfill their continuing responsibilities.

e. The requirement that retired personnel, former DoD employees, and non-active duty members of the Reserve Components use the DoD security review process specified by Reference (j).

9. MANAGEMENT AND OVERSIGHT TRAINING. Individuals designated as security managers and other personnel whose duties significantly involve managing and overseeing CUI shall receive training that addresses:

a. The designation process and the standards applicable to each designation.

b. The authorities and processes for terminating CUI status.

c. The requirements for reporting unauthorized disclosures, including when in electronic form, and the penalties that may be associated with violating established protection requirements.

d. The requirements for oversight as part of the information security program.

e. Details of the marking, dissemination, and safeguarding specifications for each type of CUI routinely used by the Department of Defense, to include:

(1) Designation standards.

(2) Use, storage, reproduction, transmission, dissemination, and destruction requirements and limitations.

(3) Access restrictions.

10. PROGRAM OVERSIGHT. The Heads of the DoD Components shall ensure that CUI education and training are appropriately evaluated during oversight activities. This evaluation shall include assessing the quality and effectiveness of the efforts, as well as ensuring appropriate coverage of the target populations. The Heads of the DoD Components shall require maintaining records of education and training offered and employee participation as they deem necessary to permit effective oversight.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ATTN	attention
CD	compact disc
CD-ROM	compact disc-read only memory
CONUS	continental United States
CUI	controlled unclassified information
DEA	Drug Enforcement Administration
DNI	Director of National Intelligence
DoD UCNI	DoD Unclassified Controlled Nuclear Information
DoDD	DoD Directive
DoDI	DoD Instruction
DoS	Department of State
DSEN	DEA Sensitive
DVD	digital video disc
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FOUO-LES	For Official Use Only-Law Enforcement Sensitive
GAO	Government Accountability Office
IAW	in accordance with
LES	Law Enforcement Sensitive
NGA	National Geospatial-Intelligence Agency
NIPRNET	Non-Secure Internet Protocol Router Network
NOFORN	not releasable to foreign nationals
PKI	Public Key Infrastructure
SBU	sensitive but unclassified
SCI	sensitive compartmented information
SNM	special nuclear material
UCNI	Unclassified Controlled Nuclear Information
UK	United Kingdom
U.S.C.	United States Code
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

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

access. The ability or opportunity to obtain knowledge of classified or controlled unclassified information.

activity security manger. The individual specifically designated in writing and responsible for the activity's information security program, which ensures that classified and controlled unclassified information is properly handled during its entire life cycle. This includes ensuring it is appropriately identified, marked, stored, disseminated, disposed of, and accounted for, as well as providing guidance on the handling of security incidents to minimize adverse effects and ensure that appropriate corrective action is taken. The security manager may be assigned responsibilities in other security disciplines such as personnel and physical security, etc.

controlling DoD office. The DoD activity that sponsored the work that generated the technical data or received the technical data on behalf of the Department of Defense and, therefore, has the responsibility for determining the distribution of a document containing such technical data. For joint sponsorship, the controlling office is determined by advance agreement and may be a party, group, or committee representing the interested activities or the DoD Components.

CONUS. U.S. territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

CUI. Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

DEA Sensitive information. Unclassified information that the DEA originates and that requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

declassification. The authorized change in the status of information from classified information to unclassified information.

distribution statement. A statement used on a technical document to denote the extent of its availability for secondary distribution, release, and disclosure without additional approvals or authorizations. A distribution statement marking is distinct from and in addition to a security classification marking. A distribution statement is also required on security classification guides submitted to the Defense Technical Information Center.

document. Any recorded information, regardless of the nature of the medium or the method or circumstances of recording. This includes any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage media.

DoD UCNI. Unclassified information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD SNM, SNM equipment, SNM facilities, or nuclear weapons in DoD custody, designated and controlled pursuant to the provisions of Reference (w).

DoS SBU. 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 provisions of the FOIA.

exemption. The basis for withholding information from public release pursuant to the provisions of the FOIA.

FOUO. A protective marking to be applied 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 provisions of the FOIA. This includes information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended. See Reference (p) for detailed information on categories of information that may qualify for exemption from public release.

information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the U.S. Government.

information security. The system of policies, procedures, and requirements established in accordance with Reference (d) to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security. The term also applies to policies, procedures, and requirements established to protect CUI, which may be withheld from release to the public in accordance with statute, regulation, or policy.

integrity. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Intelligence Community. An element or agency of the U.S. Government identified in or designated pursuant to section 403 of title 50, U.S.C., or section 3.5(h) of Executive Order 12333 (References (ae) and (af)).

international program. Any program, project, contract, operation, exercise, training, experiment, or other initiative that involves a DoD Component or a DoD contractor and a foreign government, international organization, or corporation that is located and incorporated to do business in a foreign country.

LES. A marking sometimes applied, in addition to or in conjunction with the marking "FOR OFFICIAL USE ONLY," by the Department of Justice and other activities in the law enforcement community to denote that the information was compiled for law enforcement

purposes and should be afforded appropriate security in order to protect certain legitimate government interests.

LIMITED DISTRIBUTION. A caveat used by the 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.

material. Any product or substance on or in which information is embodied.

national security. The national defense or foreign relations of the United States. National security includes defense against transnational terrorism.

need to know. A determination that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function.

network. A system of two or more computers that can exchange data or information.

page marking. Banner marking at top and/or bottom of an interior page of a document.

permanently valuable records. Records having sufficient value to warrant being maintained and preserved permanently.

records. The records of an agency and Presidential papers or Presidential records, as those terms are defined in chapters 22 and 33 of Reference (v), including those created or maintained by a U.S. Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

records management. The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. Within the Department of Defense, records management is implemented by Reference (o).

safeguarding. Measures and controls that are prescribed to protect classified and controlled unclassified information.

SCI. Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the DNI.

security clearance. A determination that a person is eligible in accordance with the standards of Reference (n) for access to classified information.

senior agency official. An official appointed by the head of a DoD Component to be responsible for direction, administration, and oversight of the DoD Component's information security

program, to include classification, declassification, safeguarding, and security education and training programs, and for the efficient and effective implementation of References (b), (d), (e) and (f) and the guidance in this Manual. Where used in reference to authorities under section 5.4(d) of Reference (d), this term applies only to the senior agency officials of the Military Departments and of the Department of Defense.

unauthorized disclosure. Communication or physical transfer of classified or controlled unclassified information to an unauthorized recipient.