

## AP3. APPENDIX 3

### CONTROLLED UNCLASSIFIED INFORMATION

#### AP3.1. INTRODUCTION

##### AP3.1.1. General

AP3.1.1.1. The requirements of the Information Security Program apply only to information that requires protection to prevent damage to the national security and has been classified in accordance with E.O. 12958 (reference (e)) or its predecessors. There are other types of information that require application of controls and protective measures for a variety of reasons. This information is known as "unclassified controlled information." Since classified information and unclassified controlled information exist side-by-side in the work environments -- often in the same documents -- this Appendix is provided as an attempt to avoid confusion and promote proper handling. It covers several types of unclassified controlled information, and provides basic information about the nature of this information and the procedures for identifying and controlling it. In some cases, the Appendix refers to other DoD Directives that provide more detailed guidance.

AP3.1.1.2. The types of information covered in this Appendix include "For Official Use Only" information, "Sensitive But Unclassified" (formerly "Limited Official Use") information, "DEA Sensitive Information," "DoD Unclassified Controlled Nuclear Information," "Sensitive Information," as defined in the Computer Security Act of 1987 (reference (j)), and information contained in technical documents.

#### AP3.2. FOR OFFICIAL USE ONLY INFORMATION (FOUO)

##### AP3.2.1. Description

AP3.2.1.1. "For Official Use Only (FOUO)" is a designation that is applied to **unclassified** information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA) (reference (g)). The FOIA specifies nine exemptions that may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. They are:

AP3.2.1.1.1. Information that is currently and properly classified.

AP3.2.1.1.2. Information that pertains solely to the internal rules and practices of the Agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an Agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding if there is no public interest in the document, and it would be an administrative burden to process the request.)

AP3.2.1.1.3. 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.

AP3.2.1.1.4. 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 protect the Government's interest in compliance with program effectiveness.

AP3.2.1.1.5. Inter-Agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.

AP3.2.1.1.6. Information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.

AP3.2.1.1.7. Records or information compiled for law enforcement purposes that:

AP3.2.1.1.7.1. Could reasonably be expected to interfere with law enforcement proceedings;

AP3.2.1.1.7.2. Would deprive a person of a right to a fair trial or impartial adjudication;

AP3.2.1.1.7.3. Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others;

AP3.2.1.1.7.4. Disclose the identity of a confidential source;

AP3.2.1.1.7.5. Disclose investigative techniques and procedures; or

AP3.2.1.1.7.6. Could reasonably be expected to endanger the life or physical safety of any individual.

AP3.2.1.1.8. Certain records of Agencies responsible for supervision of financial institutions.

AP3.2.1.1.9. Geological and geophysical information concerning wells.

AP3.2.1.2. Information that is currently and properly classified can be withheld from mandatory release under the first exemption category. "For Official Use Only" is applied to information that is exempt under one of the **other** eight categories. So, by definition, information must be unclassified in order to be designated FOUO. If an item of information is declassified, it can be designated FOUO if it qualifies under one of those other categories. This means that:

AP3.2.1.2.1. Information cannot be classified and FOUO at the same time; and

AP3.2.1.2.2. Information that is declassified may be designated FOUO, but only if it fits into one of the last eight exemption categories (categories 2 through 9).

AP3.2.1.3. The FOIA (reference (g)) provides that, for information to be exempt from mandatory release, it must fit into one of the qualifying categories **and** there must be a legitimate Government purpose served by withholding it. Simply because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information must be reviewed to see if it meets this dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of records (for example, personnel records) are not normally marked FOUO, but may still qualify for withholding under reference (g).

## AP3.2.2. Markings

AP3.2.2.1. Information that has been determined to qualify for FOUO status should be indicated by markings when included in documents and similar material. Markings should be applied at the time documents are drafted, whenever possible, to promote proper protection of the information.

AP3.2.2.2. Unclassified documents and material containing FOUO information shall be marked as follows:

AP3.2.2.2.1. Documents will be marked "FOR OFFICIAL USE ONLY" at the 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).

AP3.2.2.2.2. Pages of the document that contain FOUO information shall be marked "FOR OFFICIAL USE ONLY" at the bottom.

AP3.2.2.2.3. Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings that alert the holder or viewer that the material contains FOUO information.

AP3.2.2.2.4. FOUO documents and material transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

"This document contains information exempt from mandatory disclosure under the FOIA. Exemption(s) \_\_\_\_\_ apply."

AP3.2.2.3. Classified documents and material containing FOUO information shall be marked as required by Chapter 5 of this Regulation, with FOUO information identified as follows:

AP3.2.2.3.1. Overall markings on the document shall follow the rules in Chapter 5. No special markings are required on the face of the document because it contains FOUO information.

AP3.2.2.3.2. Portions of the document shall be marked with their classification as required by Chapter 5. If there are unclassified portions that contain FOUO information, they shall be marked with "FOUO" in parentheses at the beginning of

the portion. Since FOUO information is, by definition, unclassified, the "FOUO" is an acceptable substitute for the normal "U."

AP3.2.2.3.3. Pages of the document that contain classified information shall be marked as required by Chapter 5. Pages that contain FOUO information but no classified information will be marked "FOR OFFICIAL USE ONLY" at the top and bottom.

AP3.2.2.4. Transmittal documents that have no classified material attached, but do have FOUO attachments shall be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT."

AP3.2.2.5. Each part of electrically transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text.

AP3.2.3. Access to FOUO Information. FOUO information may be disseminated within the DoD Components and between officials of the DoD Components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other Departments and Agencies of the Executive and Judicial Branches in performance of a valid Government function. (Special restrictions may apply to information covered by the Privacy Act, reference (h).) Release of FOUO information to Members of Congress is covered by DoD Directive 5400.4 (reference (gg)) and to the General Accounting Office by DoD Directive 7650.1 (reference (ll)).

#### AP3.2.4. Protection of FOUO Information

AP3.2.4.1. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO information shall be stored in unlocked containers, desks or cabinets if Government or Government-contract building security is provided, or in locked desks, file cabinets, bookcases, locked rooms, or similar items.

AP3.2.4.2. FOUO documents and material may be transmitted via first-class mail, parcel post or -- for bulk shipments -- fourth-class mail. Electronic transmission of FOUO information (voice, data or facsimile) should be by approved secure communications systems whenever practical.

AP3.2.4.3. Record copies of FOUO documents shall be disposed of in accordance with the Federal Records Act (44 U.S.C. 33 (reference (p))) and Component records management directives. Non-record FOUO documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

AP3.2.5. Further Guidance. Further guidance on one type of FOUO information is contained in DoD 5400.11-R (reference (ww)), "Department of Defense Privacy Program."

### AP3.3. SENSITIVE BUT UNCLASSIFIED (SBU) AND LIMITED OFFICIAL USE (LOU) INFORMATION

AP3.3.1. Description. Sensitive But Unclassified (SBU) information is information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act (reference (g)). Before May 26, 1995, this information was designated and marked "Limited Official Use (LOU)." The LOU designation will no longer be used.

AP3.3.2. Markings. The Department of State does not require that SBU information be specifically marked, but does require that holders be made aware of the need for controls. When SBU information is included in DoD documents, they shall be marked as if the information were For Official Use Only. There is no requirement to remark existing material containing SBU information.

AP3.3.3. Access to SBU Information. Within the Department of Defense, the criteria for allowing access to SBU information are they same as those used for FOUO information.

AP3.3.4. Protection of SBU Information. Within the Department of Defense, SBU information shall be protected as required for FOUO information.

### AP3.4. DRUG ENFORCEMENT ADMINISTRATION (DEA) SENSITIVE INFORMATION

AP3.4.1. Description. DEA Sensitive information is unclassified information that is originated by the Drug Enforcement Administration 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 have been authorized to designate information as DEA Sensitive; the Department of Defense has agreed to implement protective measures for DEA Sensitive information in its possession. Types of information to be protected include:

AP3.4.1.1. Information and material that is investigative in nature;

AP3.4.1.2. Information and material to which access is restricted by law;

AP3.4.1.3. Information and material that is critical to the operation and mission of the DEA; and

AP3.4.1.4. Information and material, the disclosure of which, would violate a privileged relationship.

AP3.4.2. Markings

AP3.4.2.1. 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), and the outside of the back cover (if there is one).

AP3.4.2.2. In unclassified documents, each page containing DEA Sensitive information shall be marked "DEA Sensitive" top and bottom. Classified documents containing DEA Sensitive information shall be marked as required by Chapter 5, except that pages containing DEA Sensitive information but no classified information will be marked "DEA Sensitive" top and bottom.

AP3.4.2.3. Portions of DoD documents that contain DEA Sensitive information shall be marked "(DEA)" at the beginning of the portion. This applies to classified, as well as unclassified documents. If a portion of a classified document contains both classified and DEA Sensitive information, the "DEA" marking shall be included along with the parenthetical classification marking.

AP3.4.3. Access to DEA Sensitive Information. Access to DEA Sensitive information shall be granted only to persons who have a valid need-to-know for the information. A security clearance is not required. DEA Sensitive information in the possession of the Department of Defense may not be released outside the Department without authorization by the DEA.

#### AP3.4.4. Protection of DEA Sensitive Information

AP3.4.4.1. DEA Sensitive material may be transmitted within CONUS by first-class mail. Transmission outside CONUS must be by a means approved for transmission of Secret material. Non-Government package delivery and courier services may not be used. The material shall be enclosed in two opaque envelopes or containers, the inner one marked "DEA Sensitive" on both sides. Electronic transmission of DEA Sensitive information within CONUS should be over secure communications circuits whenever possible; transmission outside CONUS must be over approved secure communications circuits.

AP3.4.4.2. Reproduction of DEA Sensitive information and material shall be limited to that required for operational needs.

AP3.4.4.3. DEA Sensitive material shall be destroyed by a means approved for destruction of Confidential material.

#### AP3.5. DoD UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION (DoD UCNI)

AP3.5.1. Description. DoD Unclassified Controlled Nuclear Information (DoD UCNI) is unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities. Information is Designated DoD UCNI 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, equipment, or facilities. Information may be designated DoD UCNI by the Heads of the DoD Components and individuals to whom they have delegated the authority.

#### AP3.5.2. Markings

AP3.5.2.1. Unclassified documents and material containing DoD UCNI shall be marked as follows:

AP3.5.2.1.1. The face of the document and the outside of the back cover (if there is one) shall be marked "DoD Unclassified Controlled Nuclear Information."

AP3.5.2.1.2. Portions of the document that contain DoD UCNI shall be marked with "(DoD UCNI)" at the beginning of the portion.

AP3.5.2.2. Classified documents and material containing DoD UCNI shall be marked in accordance with Chapter 5, except that:

AP3.5.2.2.1. Pages with no classified information but containing DoD UCNI shall be marked "DoD Unclassified Controlled Nuclear Information" at the top and bottom.

AP3.5.2.2.2. Portions of the document that contain DoD UCNI shall be marked with "(DoD UCNI)" at the beginning of the portion -- in addition to the classification marking, where appropriate.

AP3.5.2.3. Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings that alert the holder or viewer that the material contains DoD UCNI.

AP3.5.2.4. Documents and material containing DoD UCNI and transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

DEPARTMENT OF DEFENSE  
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION  
EXEMPT FROM MANDATORY DISCLOSURE  
(5. U.S.C. 552 (b)(3), as authorized by 10 U.S.C. 128)"

AP3.5.2.5. Transmittal documents that have DoD UCNI attachments shall bear a statement: "The attached document contains DoD Unclassified Controlled Nuclear Information (DoD UCNI)."

AP3.5.3. Access to DoD UCNI. Access to DoD UCNI shall be granted only to persons who have a valid need-to-know for the information and are specifically eligible for access under the provisions of DoD Directive 5210.83 (reference (bb)), "Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)."

#### AP3.5.4. Protection of DoD UCNI

AP3.5.4.1. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, DoD UCNI

may be stored in unlocked containers, desks or cabinets if Government or Government-contract building security is provided, or in locked buildings, rooms, desks, file cabinets, bookcases, or similar items.

AP3.5.4.2. DoD UCNI may be transmitted by first-class mail in a single, opaque envelope or wrapping. Except in emergencies, electronic transmission of DoD UCNI shall be over approved secure communications circuits.

AP3.5.4.3. Record copies of DoD UCNI documents shall be disposed of in accordance with the Federal Records Act (44 U.S.C. 33) (reference (p)) and Component records management directives. Non-record DoD UCNI documents may be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

## AP3.6. SENSITIVE INFORMATION (COMPUTER SECURITY ACT OF 1987)

### AP3.6.1. DESCRIPTION

AP3.6.1.1. The Computer Security Act of 1987 (reference (j)), established requirements for protection of certain information in Federal Government automated information systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act) (reference (h)), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

AP3.6.1.2. Two aspects of this definition deserve attention. First, the Act applies only to unclassified information that deserves protection. Second, unlike most other programs for protection of information, the Act is concerned with protecting the availability and integrity, as well as the confidentiality of information. Much of the information which fits the Act's definition of "sensitive" falls within the other categories of information discussed in this Appendix. Some does not.

AP3.6.2. Markings. There is no specific marking authorized for designation of "sensitive" information. If the information fits within one of the other categories of information described in this Appendix, the appropriate marking requirements apply.

AP3.6.3. Access to Sensitive Information. If sensitive information falls within one of the other categories of information described in this Appendix, the specific limitations on access for the appropriate category shall be applied. If it does not,

access to the information shall be limited only to those with a valid need for such access in order to perform a legitimate organizational function, as dictated by common-sense principles of security management.

AP3.6.4. Protection of Sensitive Information. Information on DoD AIS systems that is determined to be "sensitive" within the meaning of the Computer Security Act of 1987 (reference (j)) shall be provided protection that is:

AP3.6.4.1. Determined after thorough consideration of the value and sensitivity of the information and the probable adverse impact of loss of its availability, integrity or confidentiality;

AP3.6.4.2. In compliance with applicable DoD policy and requirements for security of information within automated systems;

AP3.6.4.3. Commensurate with the degree of protection required for the category of information described in this Appendix to which it belongs (if any); and

AP3.6.4.4. Based on sound application of risk management techniques and procedures.

AP3.6.5. Further Guidance. Further guidance is found in DoD Directive 5200.28 (reference (x)), "Security Requirements for Automated Data Processing (ADP) Systems," and related publications.

## AP3.7. TECHNICAL DOCUMENTS

AP3.7.1. General. DoD Directive 5230.24 (reference (ff)) requires distribution statements to be placed on technical documents, both classified and unclassified. These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. The originating office may, of course, make case-by-case exceptions to distribution limitations imposed by the statements.

### AP3.7.2. Text of the Statements

Distribution Statement A  
Approved for public release; distribution is unlimited.

Distribution Statement B

Distribution authorized to U.S. Government agencies only; [reason]; [date].  
Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement 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 Statement 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 Statement E

Other requests for this document shall be referred to [controlling DoD office].

Distribution Statement F

Further distribution only as directed by [controlling DoD office] or higher DoD authority; [date].

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 DoD Directive 5230.25; [date].  
Controlling DoD office is [controlling DoD office].