Description of document:	Portions of the Department of Commerce Office of Security (OSY) Manual of Security Policies and Procedures, 2010
Requested date:	06-March-2010 10-May-2010 (appeal)
Released date:	12-July-2011
Posted date:	25-July-2011
Source of document:	Departmental Freedom of Information Officer Office of Privacy and Open Government US Department of Commerce 14th and Constitution Avenue NW Mail Stop H6204 Washington, D.C. 20230 Fax: 202-482-0827 Email: EFoia@doc.gov

UNITED STATES DEPARTMENT OF COMMERCE
Office of the General Counsel
Washington, D.C. 20230

JUL 12 2011

This is in response to your Freedom of Information Act (5 U.S.C. § 552) (FOIA) appeal for the release of certain documents withheld from you by the Department's Office of Security (OSY).

By letter dated March 6, 2010, you filed a FOIA request with OSY for "[t]he complete unredacted Standard Form 311 Agency Security Classification Management Program Data for the last four years," and Chapters 14, 25, 41, 44, and 45 of the Department's Manual of Security Policies and Procedures.

On April 16, 2010, OSY responded to your request by releasing four records (consisting of the requested Standard Forms 311), withholding five records in their entirety under FOIA Exemption (b)(2), and withholding three additional records in their entirety under FOIA Exemption (b)(5). By letter received by this office on May 10, 2010, you appealed OSY's initial determination to withhold those eight records.

We have reviewed your appeal and the responsive records that were originally withheld, and we have determined to grant your appeal. All eight records are being released in full, and they are enclosed with this letter.

Sincerely,

Barbara S. Fredericks
Assistant General Counsel
for Administration

Enclosures

Chapter 14 - Suspension, Revocation, and Denial of Access to National Security Information

UNDER CONSTRUCTION

Chapter 14. Suspension, Downgrade, Revocation, and Denial of Access to National Security Information

14.1. Access to National Security Information

Access to classified National Security Information (NSI) is a privilege that must be taken very seriously and guarded very closely. Whenever there is a potential threat or risk to national security, the Department of Commerce (DOC) must evaluate the risk and make a decision based on all the facts available. Security officials in the Department however, will carefully review all information presented by an applicant, employee, or other person associated with the Department, or the individual's representative on his or her behalf, and arrive at a fully validated and supported decision regarding access to national security information, based on all appropriate laws and regulations.

14.2. Derogatory Information

A. Whenever information related to Chapter 13, Security Adjudication Criteria, indicates that access to classified information by an employee or other person associated with the Department is not in the interest of national security, the supervisor, manager, or other employee of the Department shall forward that information immediately in writing through the Servicing Security Officer to the Assistant Director for Counterespionage.

B. The information will be promptly evaluated to determine the individual's eligibility or continued eligibility for access to NSI. The authority for such action is included in 5 U.S.C. § 7532. The information may also require evaluation for fitness for employment as well. If the information contained in the report is insufficient to make a determination, the Assistant Director for the Counterespionage Division (CED) may conduct or request an additional investigation, as necessary, to reach a decision concerning the impact on national security. During the inquiry, all reasonable efforts must be expended to develop the facts and circumstances to resolve pertinent security issues. The Assistant Director's determination in connection with action under 5 U.S.C. § 7532 will be made in writing and will be made a part of the investigative file.

C. Derogatory information, which may be obtained through a variety of sources and at various times during selection, appointment, and employment, shall be evaluated from both an employment and a national security perspective. Reports of investigation from investigative agencies and information concerning security issues shall be provided to the Servicing Security Officer,

for reporting to the CED. Derogatory information concerning employment and reports of employee misconduct are typically provided to the servicing human resources office.

D. Additional derogatory information obtained during the investigation will be shared between the CED and the Human Resources Office. The national security decision typically will be made prior to any employment or disciplinary decision. The CED, Human Resources Office, and Office of General Counsel will consult to determine the best course of action based on the facts obtained during the investigation.

14.3. Suspension of Access to NSI

A. In this chapter, the term "employee" shall include civil service employees, contract employees, and experts and consultants who have been granted access to NSI by the DOC.

B. Whenever the CED becomes aware of information that suggests continuation of an individual's security clearance is not in the interest of the national security, the employee's eligibility for access may be immediately suspended, pending an investigation to resolve the issues. The review and appeal procedures set forth in the following paragraphs do not apply to the suspension of an employee's access to NSI, but only to the proposal to revoke, downgrade, or deny eligibility for that access. A suspension of an employee's eligibility for access to NSI will not be indefinite. It will be reviewed by the CED every 30 days.

C. Factors to consider in making a determination to suspend an employee's access to NSI shall include all of the following:

1. The seriousness of the derogatory information developed.
2. The possible access of the employee, whether authorized or unauthorized, to classified information.
3. The opportunity, by reason of the nature of the position, for committing acts that can adversely affect the national security.

D. Pending a determination by the Assistant Director for the CED the employee may be detailed temporarily to a position that does not require a security clearance.

E. Written notification will be provided to the Security Contact. A new request (CD-79) must be submitted by the employee's supervisor through the security contact to the CED's Personnel Security Program Manager. The security contact must approve the request.

14.4. Procedures to Revoke, Downgrade, or Deny Eligibility for Access

A. When an investigation or inquiry provides information that confirms an applicant's or employee's disloyalty to the country or untrustworthiness, or raises issues of unacceptable security risk, the Assistant Director for Counterespionage may rescind, downgrade, or place restrictions on an individual's security clearance, as appropriate. Such clearance determinations for cause will be made subsequent to the suitability determination of the servicing human resources officer. The Assistant Director for CED will advise the servicing human resources officer of all security clearance actions for cause, notify the immediate supervisor or manager, and ensure that appropriate action is taken in connection with the individual's access to classified information.

B. Subject to restrictions on disclosure of NSI, an individual whose eligibility for access has been revoked, downgraded, or denied for cause shall have an opportunity to explain or to refute derogatory information developed in an investigation before such action is finalized based on the procedures outlined in the paragraphs below. The purpose of this provision is to prevent errors that might otherwise result from mistakes in identity or from mitigating circumstances that are unknown to the Office of Security (OSY). This provision does not apply to the suspension of a security clearance pending the completion of an investigation.

C. If the Assistant Director for CED makes a determination that granting eligibility for access to NSI to an applicant or employee remains an unacceptable security risk, then a proposal will be issued to revoke, downgrade, or deny the applicant's or employee's eligibility for access. Such proposals will be made in accordance with the procedures outlined below. A suitability determination conducted by the servicing human resources office concerning employment in the Department will be made independently of the proposal to revoke, downgrade, or deny an applicant or employee's eligibility for access to NSI.

D. An applicant or employee who does not meet the standards for access to NSI shall be provided with all of the following:

1. A comprehensive and detailed written explanation of the basis for that conclusion as permitted by the national security interests of the United States and other applicable laws.
2. Any document, record, and/or report upon which the proposal is based, as permitted by the national security and other applicable laws.
3. A reasonable opportunity to reply in writing to the Assistant Director for Counterespionage and to request a review of the information from which the proposal to revoke, downgrade, or deny eligibility for access was made.
4. The right to be represented by counsel or other representative at his or her own expense, for an appeal to the Deputy Director.
5. An opportunity to appear personally before an Access Review Panel (ARP), with or without representation, to give an oral response and present relevant documents, materials, and information that would explain, mitigate, or clarify the security issues concerning the proposal to revoke, downgrade, or deny eligibility for access to NSI.

E. In carrying out the provisions of this chapter, applicable regulations pertaining to the safeguarding of classified information and the handling of investigative reports shall be strictly enforced. No classified information, nor any information that might compromise investigative sources or methods or the identity of confidential informants, shall be disclosed to any employee, his or her counsel or representative, or any other person not clearly authorized access to such information.

14.5. Request for Security and Investigative Files

A. An applicant or employee who requests relevant information in his or her personnel security file and/or report of investigation shall be provided all releasable documents, records, and/or reports within 30 calendar days of the Department's receipt of the request, provided that the documents, records, and/or reports are the exclusive records of the DOC, and that they are releasable under laws pertaining to national security, privacy, freedom of information, and/or other pertinent regulations. The applicant or employee must request the security file and/or report of investigation in accordance with procedures under the Privacy Act and within 14 calendar days of receipt of the proposal to revoke, downgrade, or deny eligibility for access. Requests under

the Privacy Act for documents, records, and reports contained in the Department's Personnel Security file shall be sent to the following address:

U.S. Department of Commerce
Office of Security, Room 1067
ATTN: Privacy Act Request
1401 Constitution Ave, NW
Washington, DC 20230

B. If the proposal to revoke, downgrade, or deny an applicant's or employee's eligibility for access to NSI was based on an investigation by a non-DOC investigative agency, the applicant or employee will be required to request the Report of Investigation (ROI) directly from the investigative agency within 14 calendar days of receipt of the proposal and in accordance with Privacy Act procedures. A copy of the request to the non-DOC investigative agency must also be forwarded to the OSY.

1. The OPM generally conducts personnel security investigations in the DOC. Requests for reports of investigations conducted by the Office of Personnel Management (OPM) must be sent as a Privacy Act request to the following address:

   FOI/P, OPM-FIPC
   P.O. Box 618
   1137 Branchton Road
   Boyers, PA 16018-0618

2. If the ROI was conducted by another investigative agency, the Department will provide the appropriate address to the employee or applicant.

C. Upon notification that the individual has requested relevant information in his or her personnel security file from the OSY or the report of investigation from the appropriate investigative agency within 14 calendar days of receipt of the notice of the proposal to revoke, downgrade, or deny his/her eligibility for access to NSI, the OSY will grant a reasonable amount of time for the individual to receive the information provided in the security file or report of investigation and prepare a written response to the Assistant Director for the CED. The requester will be presumed to have received documents requested from an outside investigative agency within 30 calendar days of the date of the request for such documents unless he or she notifies the Assistant Director for Counterespionage and requests additional time to prepare his or her response.

14.6. Request to Review Proposed Revocation of Access

A. Individuals have the right to reply to the proposal to revoke, downgrade, or deny eligibility for access to NSI orally, in writing, or both, and to present information that would explain or clarify the security issues concerning the revocation, downgrade, or denial proposal. Upon receipt of the relevant information in the personnel security file from the OSY, the report of investigation from the appropriate investigative agency, or a notice of non-availability or denial of documents from either source, the applicant or employee shall have 14 calendar days to reply in writing to explain the issues and/or request a review by the Deputy Director of the proposal to revoke, downgrade, or deny eligibility for access to NSI.

B. If the OSY does not receive a request for review of the proposed revocation, downgrade, or denial of an individual's eligibility for access to NSI or does not receive a copy of the request for the individual's personnel security file or the report of investigation within 14 calendar days of receipt of the initial notice, the Deputy Director will issue a final decision to the individual revoking, downgrading, or denying their eligibility for access to NSI. A copy of this decision will be forwarded to an employee's supervisor for appropriate action.

14.7. Appeal to the Access Review Panel (ARP)

A. If the Deputy Director makes a decision to sustain the revocation, downgrade, or denial proposal, the individual shall be:

1. Provided written notice of the decision and the reasons, the identity of the deciding official, and the right to appeal the decision to an ARP, regardless of whether or not a reply to the proposal was made.
2. Given 30 calendar days from receipt of the notification to provide a written reply to the ARP established by the Director, or designee.
3. Given the opportunity to appear personally, with or without a representative, before the ARP and present relevant documents, materials, or information that would explain or clarify the security issues concerning the revocation, downgrade, or denial decision. A written record of any oral reply shall be prepared by the OSY and maintained in the individual's personnel security file. A copy of this report shall be provided to the individual.

B. If an applicant or employee appeals the decision to revoke, downgrade, or deny their eligibility for access to NSI, the Director, or designee, shall establish an ARP to review the appeal.

1. The ARP shall consist of three senior Federal Government employees who are cleared to at least the Secret level (Top Secret if needed for the particular case). Each panel member shall be at a grade level equal to or higher than the applicant/employee. Two of the panel members shall be selected from outside of the security field, one of which will be a representative of the operating unit to which the employee is assigned.
2. The Director, or designee, shall appoint members to the ARP.
3. The OSY shall provide administrative and technical support to the ARP.

C. The ARP shall convene to review the Deputy Director's decision to revoke, downgrade, or deny an individual's eligibility for access to NSI and to consider the appeal by the individual to overturn this decision. The ARP shall review all pertinent documents, records, files, inquiries, and investigations to determine the validity of the revocation, downgrade, or denial decision and to sustain or reverse the Deputy Director's decision. Decisions of the panel shall be conveyed in writing and considered final unless reviewed and reversed by the Secretary of Commerce as indicated below.

14.8. Review by the Secretary Of Commerce

A. The Director shall review the proceedings of the ARP and determine whether the record of the proceedings should be forwarded to the Secretary of Commerce (or his/her designee) for review.

B. Nothing in this process shall prohibit the Secretary of Commerce (or his or her designee) from personally exercising his or her authority to review the appeal of an applicant or employee and the decision of the ARP. In such cases, the decision of the Secretary shall be final. The review by the Secretary of Commerce is not at the discretion of the person who was denied access eligibility or whose eligibility was downgraded or revoked, but shall be determined solely by the Director.

14.9. Follow-up and Corrective Action

A. The security contact and human resources management officer shall be notified immediately of any decision to suspend, downgrade, deny, or revoke an

individual's eligibility for access to NSI. For employees, a copy of this decision shall be sent to the individual's supervisor. The Servicing Security Officer shall provide support and assistance to the individual's supervisor or program manager to ensure that appropriate action is taken to restrict the individual's access to NSI.

B. Nothing in this chapter shall limit or affect the responsibility and authority of an operating unit or Departmental office in making determinations of suitability for employment when an employee's eligibility for access to NSI has been revoked. The security contact or the CED's Assistant Director, or designee, may be consulted by the human resources officer to ensure understanding of the seriousness of any security incident or violation that leads to the decision to revoke of downgrade eligibility for access to NSI. Such a review may include describing the potential for or extent of damage to the national security. The servicing human resources manager will consult with the Office of the General Counsel, as appropriate.

14.10. Safeguarding NSI

A. In carrying out the provisions of this policy, applicable regulations pertaining to the safeguarding of classified information and the handling of investigative reports shall be strictly enforced. No classified information, nor any information that might compromise investigative sources or methods or the identity of confidential informants, shall be disclosed to any individual, to his or her counsel or representative, or to any other person not clearly authorized access to such information.

B. When the Secretary or Deputy Secretary of Commerce (or designee) makes a decision based on recommendations of the Director that a procedure set forth in this Security Manual cannot occur in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not occur. The certification by the Secretary or Deputy Secretary shall be conclusive and final.

14.11. Exceptions

A. Nothing in this chapter shall limit or affect the responsibility and power of the Secretary of Commerce to carry out any law or other Executive Order (E.O.) to deny or terminate an employee's eligibility for access to classified NSI in the interests of national security. The power and responsibility to deny or terminate access to NSI pursuant to any law or other E.O. may be exercised

only when the Secretary of Commerce or Deputy Secretary determines that the procedures prescribed in the Security Manual cannot be invoked in a manner that is consistent with national security. The decision of the Secretary or Deputy Secretary shall be conclusive and final.

B. Within the limits permitted by applicable laws, regulations, and instructions that are binding upon the Department, exceptions to the provisions of this chapter may be granted by the Director.

14.12. Reemployment of Terminated Employees

No person whose employment has been terminated by the Department under the provisions of 5 U.S.C. § 7532, E.O. 10450, as amended, E.O. 12968, E.O. 13467, or any other security or loyalty program, shall be reinstated, restored to duty, or reemployed in the Department unless the Secretary finds that such employment is clearly consistent with the interests of the national security. No person whose employment has been terminated by any department or agency, other than the DOC, under 5 U.S.C. § 7532, E.O. 10450, as amended, E.O. 12968, E.O. 13467, or any other security or loyalty program, shall be employed in the Department unless the Secretary finds that such employment is clearly consistent with the interests of the national security and unless the OPM determines that such person is eligible for such employment. The finding of the Secretary and the determination of OPM shall be made a part of the personnel security file of the person concerned.

Chapter 25 - Security Compromises, Violations, and Sanctions

UNDER CONSTRUCTION

Chapter 25. Safeguarding North Atlantic Treaty Organization Information

25.1. Purpose

The purpose of this chapter is to establish and issue the guidance, criteria, and procedures required to ensure Department of Commerce (DOC) compliance with the implementation of United States Security Authority for North Atlantic Treaty Organization (NATO) Affairs (USSAN) Instruction 1-07, "Implementation of North Treaty Organization Security Requirements."

25.2. NATO Classified Information

A. USSAN provides for U.S. implementation of NATO Security Procedures. When NATO or COSMIC precedes a classification, the material is the property of NATO, but the information remains the property of the originator. For further instruction, check with the Office of Security (OSY) and see USSAN Instruction 1-07, 3.3, "*Requirements for Access to NATO Classified Information*," and 3.5, "*Access by Non-NATO Nationals*". The determination of whether or not a U.S. document is to be released to NATO-member countries is the responsibility of the originator in compliance with the U.S. need-to-know principle. Classified information released to NATO remains the property of the originator and may not be given to any non-NATO nation or to any other international organization except by the originator.

B. NATO has four levels of classified information: Cosmic Top Secret (CTS), NATO Secret (NS), NATO Confidential (NC), and NATO Restricted (NR), which are defined as follows.

1. **Cosmic Top Secret.** This security classification applies to information whose unauthorized disclosure would result in, or could reasonably be expected to result in, exceptionally grave damage to NATO. The marking COSMIC is applied only to Top Secret documents prepared for circulation within NATO. Cosmic is a marking that, when applied to a document, signifies that both of the following conditions apply:
   a. The document is the property of NATO and may not be passed outside the organization except by the originator or with the OSY's consent; and
   b. The document is subject to the special security protection outlined in USSAN Instruction 1-07.

2. **NATO Secret (NS).** This security classification applies to information whose unauthorized disclosure could reasonably be expected to cause grave damage to NATO. NATO Secret is a designation that, when applied to a document, signifies that both of the following conditions apply:

   a. The document is the property of NATO and, if bearing a security classification, may not be passed outside the organization except under conditions outlined in USSAN Instruction 1-07, 3.5, "*Access by Non-NATO Nationals*".

   b. The document, if bearing a security classification, is subject to the security protection outlined in USSAN Instruction 1-07.

3. **NATO Confidential.** This security classification denotes information whose unauthorized disclosure could reasonably be expected to cause damage to NATO.

4. **NATO Restricted (NR).** This security classification applies to information whose unauthorized disclosure would be prejudicial to the interests or effectiveness of NATO. The United States does not have a security classification equivalent to NR, therefore, documents marked NATO Restricted will be protected in accordance with the requirements of "FOUO" information. Documents originated by NATO that are marked NR shall be marked with the following additional notation: "To be safeguarded in accordance with United States Security Authority for NATO (USSAN) Instruction 1-07." Additional detailed requirements for the protection of NR are contained in the NATO document, AC/35-D/1034, "*Supporting Document on the Security Protection of NATO RESTRICTED Information*".

C. The USSAN Instruction 1-07, "*Implementation of North Atlantic Treaty Organization Security Requirements*," is issued for compliance throughout the civilian and military elements of the Department of Defense (DOD) and all Federal departments and agencies handling NATO classified material and information. The OSY maintains a copy of this instruction.

25.3. Other NATO Information

A. **NATO Unclassified (NU).** This marking is applied to NATO information that does not require security protection. NATO Unclassified information may be handled as U.S. Unclassified information. NU shall only be used for official purpose. NU information may also carry administrative or dissemination limitation markings. The basic principles and minimum standards for handling

NU information are contained in the NATO document, C-M(2002)60, "*The Management of Non-Classified Information*".

B. **ATOMAL.** This marking is applied to either U.S. RD or FRD or United Kingdom Atomic information that has been officially released to NATO. Atomal information is classified Cosmic Top Secret Atomal (CTSA), NATO Secret Atomal (NSA), or NATO Confidential Atomal (NCA), depending on the damage that would result from unauthorized disclosure. Security provisions for ATOMAL information are contained in C-M(64)39, "*Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding Atomic Information*," and in C-M(68)41(6th Revision), "*Administrative Arrangements to Implement the Agreement between the Parties to the North Atlantic Treaty for Co-operation regarding ATOMAL Information*". U.S. personnel are directed to consult these documents directly and adhere to their provisions.

25.4. Commerce NATO Sub-registry

A. All NATO documents forwarded to the DOC are received by the sub-registry located in the DOC headquarters in Washington, DC. The sub-registry is the primary point of contact (POC) for accountability and control of all NATO documents received by the Department. For further directions, please see USSAN Instruction 1-07, 5.4, "*The Registry System*".

B. The Department has several approved control points for accountability, control, and storage of NATO material. The Servicing Security Officer or the OSY should be contacted to obtain a listing of the Departmental control points.

25.5. Security Clearance Requirements for NATO

A. Access.

1. Access to NATO classified information requires a final U.S. security clearance at the equivalent classification level (i.e., access to NATO Cosmic Top Secret requires a U.S. Top Secret security clearance and access to NATO Secret information requires a U.S. Secret security clearance). Access to NATO classified information must be limited to the minimum number of personnel who require such access to perform their assigned duties. The OSY maintains a list of all DOC personnel cleared for NATO access. Each NATO Control Point shall maintain a roster of

personnel cleared for NATO access. Verification of NATO access shall be obtained from the servicing security officer or in the OSY.

2. Although NATO Unclassified information does not require security protection, it may only be released to non-NATO nations, organizations, and individuals when such release would not be against the interest of the NATO. Any procedures considered necessary for such release will be decided independently by member nations and NATO commands and agencies.

B. Temporary Access.

1. In wartime or in periods of mounting international tension when emergency measures are required, the OSY may, in exceptional circumstances, grant temporary NATO access to personnel who do not possess the requisite security clearance, provided that such authorization is absolutely necessary, and there are no reasonable doubts regarding the trustworthiness of the person concerned. Requests for such emergency access must be fully justified and documented.
2. Whenever such emergency access is granted, a record of the authorization will be made by the OSY, which will, as soon as possible, institute the procedures necessary to fulfill the normal clearance requirements.

25.6. NATO Briefing and Debriefing

A. Before access to information classified NATO Confidential and above is granted, U.S. personnel must receive a NATO security briefing. The OSY shall conduct all NATO briefings and maintain copies of all briefing certificates for a minimum of two years from the date of briefing.

B. Uncleared personnel may be authorized access to NATO Restricted information when it is determined there is a need for such access in the performance of official duties. A personnel security clearance for such access is not required, but each person must receive a NATO security briefing.

C. A briefing shall be provided to each person who is exposed to frequent contact with representatives of countries with special security risks. A listing of "countries with special security risks" is provided in USSAN Instruction 1-07, 3.5.3.1. This list is maintained in the OSY, Counterespionage Division (CED).

D. Persons who have access to NATO classified information and who intend to travel to or through (including scheduled stopovers by air travel) countries with

special security risks, or to any destination by any form of transport that belongs to, is registered in, or managed from such a country, shall be given a thorough briefing about the security hazards of that country or geographical area before they travel. During the briefing, they will be instructed to report immediately on any occurrence that could have security implications, no matter how unimportant it may seem.

E. When access to classified NATO information is no longer required, personnel will be debriefed. All debriefings must be recorded and shall be maintained by the OSY for a minimum of two years from the date of debriefing.

25.7. Storage, Transfer and Destruction of NATO Documents

A. Storage.

1. **NATO Classified Documents.** NATO classified documents shall be stored as prescribed in USSAN Instruction 1-07. NATO documents shall not be commingled with U.S. or other documents. NATO documents may be filed in the same drawer as other non-NATO documents if they are segregated and clearly identified as NATO files. All personnel who have access to a security container that is used for the storage of NATO classified information must be cleared at the appropriate level and briefed for NATO access.
2. **NATO Restricted Documents.** NATO Restricted documents (unclassified material) may be stored in the prescribed in USSAN Instruction 1-07. NATO Restricted documents are unclassified but are protected from public access and release as "FOUO" (For Official Use Only) or "SBU" (Sensitive But Unclassified) material.
3. **COSMIC Top Secret Documents.** The DOC does not have the authority to store COSMIC Top Secret documents.
4. **Container Combinations.** The combinations of authorized security containers containing NATO classified documents shall be changed annually in accordance with USSAN Instruction 1-07.
5. **Inventory.** NATO material classified Secret and above shall be accounted for and inventoried every six months. NS sub-registries shall be inspected for compliance with security procedures by the Central U.S. Registry (CUSR) at least every 24 months or at a frequency to be determined on a case-by-case basis by the Chief, CUSR. Sub-registry self-inspection reports will be forwarded to the CUSR, with a copy retained by the sub-

registry, until the next inspection by the CUSR. Sub-registries shall inspect control points and shall retain a copy of the inspection report on file.

B. Packaging and Transmission of NATO Documents.

1. Cosmic Top Secret, NATO Secret, NATO Confidential, and all Atomal documents shall be double-wrapped in the same manner as equivalent U.S. classified documents, except that the inner wrapper shall be marked with the appropriate NATO markings. NR information shall, at a minimum, be transmitted in a single opaque envelope or wrapping. There shall be no indication that the contents are classified. NU may be transmitted in a single opaque envelope.
2. Documents classified NATO Restricted shall be packaged in the same manner as NATO Confidential and above. The outer envelope shall be marked, "Postmaster Do Not Forward. Return to Sender."
3. Requirements for the transmission of NATO classified information are contained in USSAN Instruction 1-07.

C. Destruction of NATO Information.

1. All NATO holdings must be reviewed frequently to ensure that the number of documents is kept to the absolute minimum necessary for operational purposes.
2. All NATO classified information must be destroyed in the same manner as prescribed for U.S. classified information in Paragraph 22.7 of this Security Manual. Handling and destruction of the material shall occur by appropriately cleared personnel with NATO access. Destruction certificates and control records for NS information shall be retained in the registry or office performing the destruction for a minimum of five years.

25.8. Additional NATO Security Guidance and NATO Marking

The United States Implementation of NATO Security Procedures, USSAN Instruction 1-07 Instruction, prescribes the security procedures for NATO information. The OSY maintains a copy of the instruction. Except in those instances where an intelligence source or method would be revealed, portions of U.S. documents containing foreign government information shall be marked to reflect the country or international organization of origin as well as the appropriate classification, for example, NATO-S for a NATO Secret document or UK-C for a Confidential document originated from the

United Kingdom. For additional guidance on classification markings, see Chapter 19, Marking.

Chapter 41 - Sensitive and Administratively Controlled Information

UNDER CONSTRUCTION

THIS is NOT THE Current Manual

Chapter 41 - Sensitive and Administratively Controlled Information

4101 Purpose

The Department of Commerce creates, receives, and maintains a wealth of "sensitive but unclassified" information that requires protection against unauthorized disclosure. Such information often concerns U.S. foreign relations, economic, technological, or scientific issues and requires protection from access by foreign entities seeking to further their national interests or from domestic entities seeking to gain unfair advantage in business transactions. Although not classified (i.e., national security information), such information may be exempt from disclosure by statute or regulation due to its sensitivity and shall be afforded sufficient protection to safeguard it from unauthorized disclosure. Administrative controls are usually prescribed by a specific statute or Federal regulation to protect sensitive information. Holders of sensitive information must become familiar with the guidance and apply all appropriate safeguards to protect such information from unauthorized disclosure. This chapter provides general guidance for the protection of sensitive information that is administratively controlled.

4102 Authority

This chapter is issued under the authority of DAO 200-0, Department of Commerce Handbooks and Manuals. The provisions of this chapter comply with the applicable Executive Orders, public laws, statutes, directives, and regulations issued by the Federal Government that pertain to sensitive and administratively controlled information. The following list identifies several commonly applied authorities governing the protection of sensitive information in the Department (this list is not all inclusive).

- The Freedom of Information Act, as amended (5 U.S.C. § 552).
- The Privacy Act of 1974, as amended (5 U.S.C. § 552a).
- Disclosure of Government Information (15 CFR Part 4).
- Federal Information Security Management Act of 2002 (44 U.S.C. §§ 3541-3549; PL 107-347).
- **Federal computer system security training and plan (40 U.S.C. § 11332); previously: The Computer Security Act of 1987, Public Law 100-2350).**
- Sections 9 and 214 of Title 13 of the U.S. Code, which protect from disclosure certain Bureau of the Census information.
- Invention Secrecy Act of 1951, as amended (35 U.S.C. §§ 181-188).
- The Export Administration Act of 1979, as amended (50 U.S.C. App. § 2401 et seq.).
- Department of Defense regulations regarding the identification of records as "For Official Use Only" (FOUO) (32 CFR Subpart D).
- Economic espionage (18 U.S.C. § 1831).
- Theft of trade secrets (18 U.S.C. § 1832).
- Disclosure of confidential information generally (18 U.S.C. § 1905).
- Utilization of Federal technology (concerning transfer of technology) (15 U.S.C. § 3710).
- Unauthorized disclosure of information (26 U.S.C. § 7213).
- Prohibition on release of contractor proposals (41 U.S.C. § 253b (m)).
- Executive Order 12600, Predisclosure Notification Procedures for Confidential Commercial Information, 52 Fed. Reg. 23781 (June 25, 1987).
- Department Administrative Order 205-12, Public Information.

- Department Administrative Order 205-14, Processing Requests under the Freedom of Information Act.

4103 Application OK

Administrative controls are necessary to preclude the loss or compromise of sensitive information. Due to the extensive types of sensitive information in the Department, sub-categories of sensitive information will not be identified in this chapter. Each head of an operating unit or departmental office is responsible for developing and implementing in writing additional administrative controls, as required, to protect sensitive information in their respective unit or office. For guidance on the administrative controls required to protect sensitive information not covered in the Security Manual, individuals should consult the originator of the material to determine what protective measures are required.

4104 Roles and Responsibilities OK

A. The Director for Security shall:

1. Issue policies, procedures, and guidance necessary to protect and safeguard sensitive and administratively controlled information;

2. Assist the heads of operating units or departmental offices to implement the provisions of this chapter;

3. Assist the heads of operating units to coordinate the protection of sensitive information involving more than one department or agency, as necessary; and

B. Heads of Operating Units or Departmental Offices shall:

1. Implement the provisions of the Security Manual to protect and safeguard sensitive and administratively controlled information;

2. Issue additional policies, procedures, and guidance, as necessary, to protect and safeguard sensitive and administratively controlled information in their respective organizations;

3. Ensure that employees in their respective organizations are provided the training necessary to protect and safeguard sensitive and administratively controlled information.

C. The Office of the Chief Information Officer shall be responsible for:

1. Issuing policies, procedures, and guidance for the accreditation of sensitive information technology (IT) systems used in processing and electronically transmitting sensitive information; and

2. Coordinating with the Office of Security in reporting security violations or infractions involving unauthorized disclosure of sensitive and administratively controlled information.

D. Supporting security officers shall:

1. Assist their operating unit in the application of the procedures of this chapter;

2. Assist their operating unit with periodic evaluations of the categories of sensitive information generated by their organization and in the application of any additional protective measures that apply to this information; and

3. Provide guidance and awareness materials to employees on the proper handling of sensitive information.

E. Employees shall:

1. Protect sensitive or administratively controlled information in their possession and return such information to the appropriate departmental office prior to terminating employment or association with the Department or when the information is no longer needed in the performance of assigned duties;

2. Become familiar with, and adhere to, guidance provided in the Security Manual to protect sensitive information; and

3. Ensure they are knowledgeable of applicable statutes, policies, procedures, or regulations issued by an operating unit or departmental office in order to protect sensitive information.

4105 "For Official Use Only" Information

A. Use of For Official Use Only in the Department of Commerce.

1. Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public because there is a sound legal basis for withholding the information under a specific statute shall be designated "For Official Use Only" (FOUO). Information not expressly protected by a statute shall not be designated FOUO. In addition, FOUO is not authorized as a less stringent form of classification to protect national security interests that are not classified. Examples of such statutes exempting sensitive information from disclosure to the public include the Export Administration Act, the Invention Secrecy Act, Title 13 of the U.S. Code concerning census information, Title 18 of the U.S. Code concerning Trade Secrets, and the Freedom of Information Act.

2. The FOUO designation may be applied by any secretarial officer, head of an operating unit, senior departmental official, or program manager who processes, handles, or maintains information that may be withheld from public disclosure under appropriate laws. The FOUO designation may also be applied to other information that has been determined by a Department of Commerce official to be sensitive (e.g., national economic policy not yet publicly released, pending reorganization plans, or sensitive travel itineraries).

3. The prior application of FOUO markings is not a conclusive basis for withholding a record that is requested under the FOIA. When such a record is requested, the information in it shall be evaluated to determine whether there is a sound legal basis for withholding the record under one or more FOIA exemptions. For specific determinations regarding the application of the Freedom of Information Act to sensitive information, contact the Department's FOIA Officer. Assistance concerning the application of FOIA laws may also be obtained from the relevant operating unit's FOIA officer or from the Department's Office of the Assistant General Counsel for Administration.

4. In order for specific information to be identified as FOUO, the following criteria must be met:

a. **Category Test.** Information under consideration for identification as FOUO information must be:

(1) Unclassified (i.e., not Restricted Data, Formerly Restricted Data, or national security information);

and

(2) Exempt from public release based on an appropriate statute.

b. **Sensitivity Test.** Information under consideration for identification as FOUO must, in the judgment of the originator, be information where:

(1) There is a legitimate Government interest in restricting disclosure; and

(2) Protection of the information from disclosure outweighs the public's right to know this information.

B. Designating FOUO Information. Information being considered for the FOUO designation in the Department of Commerce must be unclassified and should fall under one of the categories noted below.

1. Information exempted from disclosure by statute, such as census information (Title 13), patent information (35 U.S.C. §§ 181-188), or other categories of sensitive information.

2. Information and material originated within or furnished to the Department which fall under one or more of the following exemption criteria of the Freedom of Information Act noted in 5 U.S.C. § 552.

3. Information specifically exempted from disclosure by another statute, provided that the statute requires the matters be withheld from the public in such a manner as to leave no discretion on the issue, or establishes particular criteria for withholding or refers to particular types of matters to be withheld (such as Section 12(c) of the Export Administration Act, which protects information concerning export license applications).

4. Information that concerns trade secrets and commercial or financial information obtained from a person and privileged or sensitive.

5. Investigation records or information compiled for law enforcement purposes, but only to the extent that the production of such records or information:

a. Could reasonably be expected to interfere with enforcement proceedings;

b. Would deprive a person of a right to a fair trial or an impartial adjudication;

c. Could reasonably be expected to constitute an unwarranted invasion of personal privacy;

d. Could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source;

e. Would disclose investigative techniques and procedures for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; or

f. Could reasonably he expected to endanger the life or physical safety of any individual.

6. Operations Security (OPSEC) surveys, counterintelligence inquiries and operational records, compliance review results, or security inspection reports identifying security risks or vulnerabilities.

7. Information that contains detailed technical information about the security of an Information Technology (IT) system, its security requirements, and/or the controls planned, recommended, or implemented. This information may include, but is not limited to, the system security plan, risk analysis, contingency and disaster recovery plans, certification and accreditation testing and results, internal control reviews, and verification reviews.

8. Information that is determined by a Secretarial Officer of the Department of Commerce to be unusually sensitive (e.g., national economic policy not yet publicly released, pending reorganization plans, sensitive travel itineraries, or administrative investigations).

C. Marking FOUO Information.

1. A document containing unclassified, sensitive information shall be marked "For Official Use Only" (FOUO) on the bottom of the front cover (if any), on each interior page that contains FOUO information, and on the outside of the back cover (if any). Each paragraph containing FOUO information shall be marked as such. Exceptions to this policy may occur only if specific guidelines are utilized to protect the sensitive information from unauthorized disclosure such as census information protected under Title 13 of the U.S. Code. In all cases, the recipients of FOUO information shall be made aware of the status of such information and that special handling may apply (see paragraph 4106 B.).

2. Operating units may wish to identify a record as FOUO at the time of creation so as to provide notice of FOUO content and thereby facilitate review when a record is requested under the FOIA. Records requested under the FOIA that do not bear such markings shall not be assumed to be releasable without examination for the presence of information that requires continued protection and qualifies as exempt from public release.

3. When a document contains both classified and FOUO information, the classified markings shall be applied at the top and bottom of each page with the highest security classification of information appearing on each page (see Chapter 20, Identification and Marking). An individual page that contains FOUO information but no classified information shall be marked "For Official Use Only" at the top and bottom of the page. Individual paragraphs shall be marked at the appropriate classification level as well as unclassified or FOUO, as appropriate.

4. To ensure the FOUO information will be protected after a classified document has been declassified, the following annotation should be made in the lower right hand corner of the document:

This document becomes "For Official Use Only" upon declassification.

5. FOUO material transmitted outside the Department of Commerce may require the application of an expanded marking to explain the significance of the FOUO marking. This can be accomplished by typing or stamping the following statement on the record prior to transfer:

Example:
This document contains information exempt
From mandatory disclosure under the [list reference]
Exemption(s) _____ apply.
Determined by: _____ Date: _____

6. FOUO information transmitted by electronic or facsimile media shall be clearly marked before the beginning of the text and, if necessary, throughout the text to identify the part of the message that is FOUO.

D. Transmitting FOUO Information.

1. FOUO information may be disseminated within Department of Commerce operating units and departmental offices to conduct official business of the Department. Recipients shall be made aware of the status of such information, and transmission shall be by means that preclude unauthorized public disclosure. Transmittal documents shall call attention to the presence of FOUO attachments or enclosures. Within a Department of Commerce facility, the Form CD-494, Sensitive Information Cover Sheet, shall be used to cover FOUO documents transmitted between offices.

2. Department of Commerce holders of FOUO information are authorized to convey such information to officials in other Departments or agencies of the Executive and Judicial branches to fulfill a governmental function, except to the extent prohibited by the Privacy Act. Records thus transmitted shall be marked "For Official Use Only," and the recipient shall be advised that the information may qualify for exemption from public disclosure based on a FOIA exemption or other appropriate statute or regulation and that special handling instructions may apply.

3. Transmittal documents containing FOUO information require special markings to call attention to the presence of FOUO attachments or enclosures and shall be transported in a manner that prevents unauthorized disclosure of the contents.

4. Before sending FOUO information outside of an office or the Department, all such documents shall be enclosed in a single, opaque envelope or wrapping. The envelope shall not bear any FOUO markings. If additional protection is required, senders may also opt to double-wrap the material, plainly marking both sides of the inner envelope with the marking, "For Official Use Only." Both envelopes shall be fully addressed to the appropriate official by name and title. The outer envelope shall not bear any FOUO markings. When not commingled with classified information, FOUO material may be sent via first-class mail or parcel post although, when practicable, a courier is the preferred method for local delivery.

5. For release of FOUO information to the Legislative Branch, officials should consult the Office of Legislative Liaison for the Department or the legislative liaison for the operating unit.

6. Electronic transmission of FOUO information is authorized for the conduct of official business. Methods of electronic transmission include voice discussions over a public telephone line, sending documents to or from a non-secure facsimile (fax) machine, or data transmission using a non-secure computer network (e.g., e-mail). FOUO information should be encrypted in transmission because there is no expectation of protection of information sent over an unprotected network; however, a strict prohibition of such transmittal could seriously restrict the efficient operation of an operating unit or office. Department of Commerce officials must realize that non-encrypted transmissions may be monitored, intercepted, and modified. The following guidelines must be followed when transmitting FOUO information through non-secure electronic systems.

a. FOUO information may be transmitted electronically if the originator of the information does not prohibit the transfer of the FOUO information by such means. If necessary, the sender will consult with the originator of the information to determine if it is permissible to transmit the information electronically through an unprotected network.

b. FOUO information normally should not be discussed over the telephone or transmitted electronically through an unprotected computer network unless the risk of loss or compromise of that information has been

evaluated and the sender has determined the benefit of sending the information outweighs the risk of its loss or compromise.

c. FOUO information may be transmitted over a non-secure facsimile (fax) machine without encryption; however, it is incumbent upon the sender to verify the fax number to which the material is being sent. Verification of the number requires the sender to contact the office by telephone and verify the correctness of the fax number. In addition, arrangements must be made for an authorized person to stand by the fax machine and promptly receive the transmission, thus precluding unauthorized disclosure or dissemination.

d. The sender must verify the identification of the recipient's phone/fax number or e-mail/IP address before sending the information or calling the individual. The sender should not leave FOUO information in a voice message on a caller's answering machine.

e. If the information reveals vulnerabilities or information that could potentially cause damage to the originator, sender, or receiver if lost or compromised, the sender must evaluate the risk of transmitting the information through an unprotected network and proceed only upon concluding that the benefit of transmission exceeds potential loss or compromise.

7. Since requirements for the security of unclassified, sensitive information vary for different applications, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses to confidentiality, integrity, and availability of such information. The overall security level for a particular information system must be chosen to provide an acceptable level of security for the given application and environment in which the system is utilized. Technical requirements for specific levels of security can be obtained from current standards in the Federal Information Processing Standards (FIPS) series of publications issued by the National Institution of Standards and Technology (NIST) and NIST Special Publications for Information Security.

E. Safeguarding and Storing FOUO Material.

1. During normal working hours, FOUO information must be stored in an out-of-sight location to ensure visitors and other unauthorized persons cannot obtain access to it. FOUO information must not be left unattended.

2. During non-duty hours, FOUO material shall be stored to prevent unauthorized access. Such material may be stored with other unclassified material in unlocked files cabinets, desks, or bookcases when normal Federal Government or Government-contractor internal building security measures are adequate during non-duty hours (i.e., guard force, restricted access, etc.). When internal security measures are not available or when office spaces can be accessed after hours by authorized but unescorted personnel who do not have a need-to-know (i.e., custodial staff, maintenance personnel, etc.), FOUO materials shall be stored in a locked room, filing cabinet, or other appropriate container.

F. Destruction of FOUO Material.

1. The originator of FOUO information or other competent authority shall be held responsible for the continued review and prompt removal of FOUO markings when the information no longer requires protection from public disclosure. When FOUO status is terminated, all known holders shall be notified, to the extent practicable. Upon notification, holders of such information in the Department shall efface or remove the FOUO markings, but records in file or storage do not need to be retrieved solely for that purpose.

2. FOUO material shall be destroyed by any means that prevents the disclosure of its contents. Burning is not required for the destruction of FOUO material, unless specified by instruction of the originator. Non-record copies of FOUO materials may be destroyed by tearing each copy into pieces to prevent reconstructing the information, and placing the strips in regular trash receptacles. When local circumstances or experience indicates that this destruction method is not sufficiently protective of FOUO information, local authorities may direct other methods for destroying the information; however, due consideration must be given to the additional expense balanced against the degree of sensitivity of the FOUO information contained in the records. Crosscut shredders (utilized for destruction of classified material) or the plain, "unclassified" burn bags may be used for this purpose.

3. Records copies of FOUO documents shall be disposed of in accordance with the instructions provided by the Department's Records Control Officer or by the records control schedule of a particular operating unit or departmental office.

G. Reproduction of FOUO Information. FOUO information may be reproduced without obtaining specific approval of the originator, unless otherwise noted on the document. Copies must be marked and protected in the same manner as the original. Copy machine malfunctions must be cleared with all paper paths checked for any remaining material.

H. Mishandling, Loss, or Unauthorized Disclosure of FOUO Material.

1. The unauthorized disclosure of FOUO information does not constitute an unauthorized disclosure of Department of Commerce information classified for security purposes. Appropriate administrative action shall be taken, however, to determine responsibility for the unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those persons responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act or other specific statute may also result in civil and criminal sanctions against responsible persons.

2. Any person who has knowledge or suspects a violation or infraction involving the mishandling, loss, or unauthorized disclosure of FOUO information shall:

a. Take custody of the information if necessary and safeguard it in an appropriate manner; and/or

b. Promptly notify their security contact or servicing security officer that there has been an unauthorized disclosure of FOUO information.

3.. The security contact shall ensure that the originator of the information and the servicing security officer are notified and action is taken to prevent further occurrence.

I. Denial and Appeal for Release of FOUO Information.

1. Several of the operating units generate, process, handle, or store sensitive information that falls under one of the FOUO designations identified in paragraph 4105 B. above. Each head of an operating unit or departmental office shall be responsible for providing guidance to individuals in their respective organizations for protecting sensitive information. Each employee shall ensure that sensitive information is afforded the appropriate level of protection and is not released to the public if protected by a FOIA exemption or other statute.

2. When FOUO information is requested for release to the public, the information shall be evaluated to determine whether there is a sound legal basis for withholding the information under one or more FOIA exemptions or other statute. Any reasonably segregable portion of a record shall be provided to the requester after deletion of the

exempted or protected portions. The amount of information deleted shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by a FOIA exemption or other statute or regulation under which the deletion is made. If technically feasible, the amount of information deleted shall be indicated at the place in the record where such deletion is made.

3. Throughout the Department of Commerce, selected officials have been delegated the authority to initially deny requests for records in their respective units for which they are responsible. The list of such denial officials is provided in 15 CFR, Part 4, Appendix B, Officials Authorized to Deny Requests for Records Under the Freedom of Information Act, and Requests for Records and Requests for Correction or Amendment Under the Privacy Act.

4. When an initial request for a record has been denied in whole or in part, or has not been timely determined, or when a requester has received an adverse initial determination under the Department's FOIA regulations, the requester may file a written appeal, which must be received by the Assistant General Counsel for Administration within thirty calendar days after the date of the written determination or, if there has been no determination, on the last day of the applicable time limit (see 15 CFR § 4.10).

4106 Protection of Other Sensitive Information

A. Departmental offices and operating units that generate or maintain sensitive information must protect such information in accordance with Federal laws, regulations, or operating unit specific policy. In addition, several Department of Commerce operating units have a memorandum of understanding (MOU) with other agencies regarding the protection of specific types of sensitive information. For specific policies and procedures protecting such sensitive information or if a conflict arises in reference to an MOU or other agreement, personnel should consult with the operating unit or departmental office originating the information to clarify applicable policies and procedures. Such information may require a greater level of protection than that required for FOUO information.

B. The authority, handling, storage, safeguards, and disposal for information in the following categories are described in the Department's or the respective operating unit's guidance for that specific information. Questions concerning proper use and protection of such information should be made to the appropriate Department of Commerce office that maintains and oversees that information. For example, questions concerning the protection of procurement information should be referred to the Office of Acquisition Management; questions concerning protection of official personnel information should be referred to the Office of Human Resources Management.

1. **Procurement Information.** Departmental procurement information including proprietary information, contract proposals, and source selection information shall be protected from unauthorized disclosure as specified in the Commerce Acquisition Regulation (CAR) and Federal Acquisition Regulation (FAR). Individuals who handle this information in the course of their official duties shall review the relevant sections of the CAR and FAR to be familiar with the requirements for handling sensitive procurement information.

2. **Personnel Information.** Personnel information includes, but is not limited to, leave records, information contained in official personnel files, social security information, reports of investigations, employee addresses and telephone numbers, benefit information, medical records, performance appraisal data, financial information, and records of disciplinary actions. Information relating to personnel or personnel management in the possession or control of the Department may be required to be withheld from disclosure under the Privacy Act. The Freedom of Information Act may also exempt such information from public disclosure. Additional guidance on handling personnel information may be obtained from the Director, Office of Human Resources Management or a servicing human resources management office.

3. **Travel Information.** Travel itineraries and related documents may be sensitive and may require handling and safeguarding in some circumstances. An example would be travel information which, if disclosed, may jeopardize the physical safety of departmental personnel, facilities, or their dependents as well as U.S. citizens overseas when there is an assessed terrorist threat to the person traveling on official business or a general threat to American citizens present at locations to be visited. In most cases, travel related information is no longer sensitive when travel has been completed.

4. **Personnel Investigative Information.** Personnel security files, background investigations, credit reports, and other investigative records shall be safeguarded based on guidance in the Department's Privacy Act Systems of Records. Personal information in such records and files also will be subject to protection from unauthorized release by the Freedom of Information Act (FOIA).

5. **FOIA Exemptions.** Other information held by Department of Commerce personnel that is subject to the Freedom of Information Act shall be protected from unauthorized disclosure.

4107 Information Technology Security Related Material

The Office of the Chief Information Officer (OCIO) has determined that information that contains detailed technical information about the security of an Information Technology (IT) system, its security requirements, and/or the controls planned, recommended, or implemented, requires protection from unauthorized disclosure. Sensitive IT security related information shall be marked FOUO to provide protection against unauthorized disclosure (see paragraph 4105B.7.). This information includes, but is not limited to, the system security plan, risk analysis, contingency and disaster recovery plans, certification and accreditation testing and results, internal control reviews, and verification reviews. Other guidance for protection of IT information can be found in the OCIO's Information Technology Security Manual (***obtain web site reference***).

4108 Foreign Relations/Foreign Affairs Information

Unless classified for national security reasons, the following information receive from other departments or agencies is sensitive and should be handled and safeguarded as FOUO information.

- Information which, if improperly released, could have a negative impact on foreign policy or relations including negotiations between governments, private businesses, international financial and monetary institutions, or official representatives, including deliberative process documents and attorney-client communications.

- Information considered critical to the Department's foreign affairs mission including policy or positions for bilateral or multilateral negotiations, consultations, or international agreements.

- Information in connection with trade agreements, anti-dumping and countervailing duty cases.

4109 "Sensitive But Unclassified" Information

A. The term, "Sensitive But Unclassified" (SBU) replaced the term, "Limited Official Use" (LOU), previously used by the Department of State for privileged or proprietary information. All requirements concerning the SBU program can

be found in the U.S. Department of State Foreign Affairs Manual, Section 12, FAM 540 (http://foia.state.gov/REGS/Search.asp).

B. SBU is not a term used for the identification of classified national security information. The term, SBU, provides administrative handling instructions within the Department of State. There are occasions where such material is handled within the Department of Commerce. Access to SBU information in the Department of Commerce shall be limited to protect it from unauthorized disclosure.

C. Examples of SBU information include: personal, medical, financial, investigatory, visa, law enforcement, or other information offered under conditions of confidentiality which may arise in the course of deliberative process (such as attorney-client privilege or work product), or information arising from the advice and counsel of subordinates to policy makers. If released to unauthorized persons, SBU could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations.

D. In certain rare situations, some SBU information will require a distribution restriction. If specific SBU information warrants a "higher level of protection" as noted in the U.S. Department of State Foreign Affairs Manual, Section 12, FAM 544, distribution restrictions should be used. Custodians of SBU information must decide whether specific information identified as SBU warrants a higher level of protection provided by the use of a secure fax, secure phone, or other encrypted means of communications.

E. If SBU information is discovered during an after-hours security inspection in areas accessible to unauthorized personnel, the material shall be secured. Although a security incident report for unsecured SBU information normally is not issued, the servicing security officer shall be notified. However, it is recommended that the servicing security officer contact the offending employee's supervisor to report the incident to ensure that the employee does not repeat this action in the future.

F. Personnel should refer to the U.S. Department of State Foreign Affairs Manual, Section 12, FAM 540, for additional guidance regarding SBU information.

4110 "Limited Official Use" Information

"Limited Official Use" (LOU) is a designation used by the Department of Justice and its bureaus. The term is generally equivalent to the Department's FOUO. Such information should be protected accordingly unless additional protection is given to the information.

Chapter 44 - Emergency Preparedness

UNDER CONSTRUCTION