Chapter 21 - Access and Dissemination

2101 Access to Classified Information

A. Federal employees are not automatically granted access to classified information. An employee is eligible for access to classified information only when the employee has been determined to be trustworthy by an appropriate investigation and access is essential to the accomplishment of lawful and authorized government purposes. The number of people cleared and granted access to classified information shall be maintained at the minimum number consistent with operational requirements and needs.

B. The heads of operating units must ensure that only authorized persons obtain access to classified information. No employee has a right to gain access to classified information solely by virtue of title, position, or level of security clearance. Before classified information is disclosed, the holder must verify the recipient's identification and security clearance through their operating unit's servicing security officer or security contact, determine the recipient's need to know, and advise the recipient of the classification level of the information. In addition, the final responsibility for determining whether an individual obtains access to classified information rests with the individual who has possession, knowledge, or control of the information and not with the prospective recipient.

C. Employees approved for access to classified information must sign the Classified Information Non-disclosure Agreement, SF-312, prior to the formal granting of a security clearance, and agree to be bound by statutes concerning the protection of classified information.

2102 Downgrade or Termination

A. The head of an operating unit or the Director for Security may determine that an individual no longer requires access to classified information in the performance of official duties or contractual obligations, or that the individual requires access at a lower level. When an individual (employee, contractor, etc.) no longer needs access to a particular classification level, the level should be adjusted or downgraded to the classification level required for the performance of the individual's duties and obligations, or access should be withdrawn. The administrative adjustment, downgrade, or withdrawal of an individual's security clearance shall be made in writing to the individual with a copy to his/her supervisor (or Contracting Officer's Technical Representative, if a contractor). The administrative downgrade or withdrawal of an individual's security clearance does not prejudice the person's eligibility for a future security clearance. A copy of all administrative changes to the classification level required for a particular position must be forwarded to the servicing human resources officer so that the

position record can be updated accordingly.

B. The Director of Security, or his designee, shall suspend or revoke a security clearance when the clearance or access is no longer consistent with the interests of national security. Procedures for revocation of a security clearance for cause are prescribed in Chapter 14, Suspension and Revocation of Access to National Security Information.

C. Upon termination of a security clearance, the holder shall receive a formal security debriefing describing the continuing responsibility to protect the national security information to which the individual had access. The reverse of the Classified Non-Disclosure Agreement, CD-312, shall be completed upon debriefing. In addition, a copy of the sanctions under Title 18 of the U.S. Code shall be given to the debriefed employee to re-emphasize criminal prosecution penalties for unauthorized disclosure of classified information.

D. Classified information (in any form), to include extra copies, is not personal property and may not be removed from the Government's control by any departing employee or contractor. The operating unit security contact shall ensure that all debriefed personnel have accounted for all classified information in their possession and transferred it to an authorized custodian. The servicing security officer shall verify that the departing individual does not have any classified documents or security containers still assigned to them.

2103 Restrictions

A. Classified information may be discussed under the following four conditions:

1. The recipient of the classified information has a current security clearance at the appropriate level;

2. The holder of the classified information has verified the identification of the intended recipient;

3. The holder of the classified information has obtained a need-to-know by the recipient; and

4. The discussion must be held in appropriately cleared Federal Government or contractor facilities to preclude unauthorized disclosure of classified information.

B. Classified information may not be removed from official premises without proper authorization. An official or employee leaving agency service may not remove classified information from the Department's control.

C. Classified information shall remain under the control of the originating agency or its successor in function.

Operating units in the Department shall not disclose information originally classified by another agency without its authorization. Persons authorized to disseminate classified information outside the Executive Branch shall assure the protection of the information in a manner equivalent to that provided within the Executive Branch.

D. Discussing classified information in homes, public places, or on public conveyances, or anywhere unauthorized persons have access is strictly prohibited. Employees or other individuals cannot retain or utilize classified information for their private use.

E. Secure Telephone Units (STU III), Secure Telephone Equipment (STE), and approved secure facsimile (fax) equipment must be used for the telephonic and data transmission of classified information. Specific questions regarding the use of the telecommunication systems for transmission of classified information should be directed to the Department's Communications Security (COMSEC) Custodian in the Office of Security. Standard telephones shall not be used for classified discussions.

F. Each operating unit in the Department shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

G. Except as otherwise provided by statute, E.O. 12958, directives implementing this order, or by direction of the President, classified information originating in one agency shall not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. The Director for Security may waive this requirement for specific information originated within that agency. Prior consent is not required when operating unit refer records for declassification review that contain information originating in several agencies.

2104 Certification of Security Clearance

Any employee, contractor, expert, or consultant of the Department of Commerce who has a need to visit or certify clearance information to another agency or facility, must initiate the Visit Authorization and Security Clearance Certification Request, Form CD-414. The form must be completed, signed by the servicing security officer and submitted to the agency to be visited. The form shall be submitted within 10 working days (or sooner) of the visit or period of clearance certification. However, some agencies or government facilities require the use of their own form for visits to their facilities. The individual coordinating the clearance certification

request should verify the method acceptable to other agencies prior to the visit.

2105 Access by Historical Researchers and Former Presidential Appointees

A. Persons who are engaged in historical research projects or who have previously occupied policy-making positions appointed by the President may be granted authorized access to classified information provided the head of the operating unit with jurisdiction over the information:

1. Makes a written determination that access is consistent with the interests of national security and forwards a copy of this determination to the Director for Security;

2. Takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with E.O. 12958 and the Security Manual;

3. Obtains written nondisclosure agreements from the requester to safeguard the information to which they are given access in accordance with the Security Manual;

4. Obtains written consent to a review by the Department of Commerce of the requester's resultant notes and manuscripts to determine that no classified information is contained in the material; and

5. Limits access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

B. Historical researchers and former Presidential appointees will provide the Office of Security with a detailed description of their research. Access will be granted to these individuals for a limited period of time. Requests for access must be made in advance and approved by the Director for Security. Access will be granted only if a compelling need exists and it is in the Department's best interest. The information requested shall be clearly identified so that it can be located and compiled with a reasonable amount of effort. If the access requested by historical researchers or former Presidential appointees requires the rendering of services for which fair and equitable fees may be charged, the requester shall be so notified.

C. The provisions of Section III, National Security Information, apply only to classified information originated by Department of Commerce, or information that is now in the sole custody of the Department; otherwise, the

researcher should be referred to the classifying agency. Operating units providing information under this section must maintain custody of classified information at a Departmental facility.

2106 Access by Foreign Nationals, Foreign Governments, International Organizations, and Immigrant Aliens

A. If the head of an operating unit indicates a need to provide access to foreign nationals, the sponsoring officer must consult with the servicing security officer for a final decision.

B. Foreign nationals employed by the Department who meet the requirements set forth in Chapter 11, Investigative Processing, may be granted access to classified information originated by the Department. Access shall be granted only for the specific classified project to which they are assigned and only after they have met the requirements set forth in Section II, Personnel Security, of this manual.

C. Dissemination of classified military information to foreign governments and international organizations is governed by the National Disclosure Policy (NDP-1). The Department of State determines the classified foreign relations information that will be disseminated to foreign governments. The disclosure of national security information to foreign governments and international organizations must meet the following criteria:

1. The disclosure supports U.S. foreign policy;

2. The national security of the U.S. permits disclosure;

3. The foreign recipient has the capability and intent to protect the information;

4. A clearly defined benefit to the U.S. government outweighs the risks involved; and

5. The release is limited to that information necessary to satisfy the U.S. Government's objective in authorizing the disclosure.

D. The Director for Security shall approve any recommendation to release classified information to a foreign government or international organization.

2107 Dissemination of Commerce Classified Information

A. The head of each operating unit or their designee is responsible for providing direct control of the dissemination of classified information received or generated in their offices.

B. The head of an office who hosts or convenes a meeting (conference, symposium, seminar, exhibit, convention, scientific, or technical gathering) at which classified information is disclosed must:

1. Verify the security clearance and need-to-know of each person attending the meeting;

2. Identify attendees before admitting them to the meeting room; and

3. Advise persons (i.e., speakers) who will present classified information of any limitations on their presentation that may be necessary because of the level of security clearance and need-to-know of attendees. The speaker is responsible for seeking such guidance and for keeping classified disclosures within the prescribed limits. He/she is also responsible for advising the audience of the classification level of, the authority for, and the duration of the classification of the information disclosed, including any special marking, storage, or safeguarding requirements.

C. Employees who attend meetings where classified information is disclosed shall obtain adequate information on the level and duration of, and authority for, classification of the information disclosed in order to provide appropriate derivative classification to any documentation resulting from the meetings.

D. Notes, minutes, summaries, recordings, proceedings, reports, etc., of the classified portions of the meeting are referred to as working papers. The materials shall be safeguarded and controlled throughout the duration of the meeting. At the conclusion of the meeting, the materials shall be forwarded, if needed, to attendees by approved secure transmission methods.

E. Physical and technical security controls shall be established appropriate to the classification and sensitivity of the information to be discussed. Due to inherent security threats, classified meetings or classified sessions of a meeting shall be held only in U.S. Government or cleared contractor facilities when possible. When not possible, arrangements to address physical and technical security controls shall be coordinated with the Office of Security.

2108 Dissemination of Other Agency Information

Classified information originated in another agency shall be disseminated outside of the Department of Commerce only with the consent of the originator. This is commonly known as the "Third Agency Rule."

Consent must be maintained in writing as a matter of record. This restriction does not apply to additional distribution within the Department or distribution to contractors who are U.S. citizens and require the information in performance of contracted services (unless the documents are marked "PROPIN" (Proprietary Information)).

2109 Dissemination Outside the Executive Branch

Department of Commerce classified information can be made available to persons outside the Executive Branch provided: 1) they are engaged in historical research projects or previously have occupied policy-making positions and were appointed by the President; or 2) the information is necessary for their performance of a function related to a contract or other agreement with the U.S. Government; or as provided below.

A. United States Congress.

1. Classified information originated by the Department of Commerce shall be released to the U.S. Congress, its committees, members, and staff representatives when necessary in the interests of the national security, and as authorized by the Secretary or the head of an operating unit. Such release shall coincide with the provisions of Department Administrative Order 218-1, Legislative Activities. Proposals to transmit classified information to the U.S. Congress must be reviewed by the servicing security officer, the Director of Security, and the Office of General Counsel, prior to release.

2. Commerce personnel who appear as a witness before a Congressional committee shall request that classified testimony be given in executive session only, that any record of such testimony be identified as classified and not appear in any document subject to public inspection or availability, and shall obtain the assurance of the committee chair that everyone present has an appropriate security clearance or agrees to safeguard the classified information from public disclosure. By virtue of their elected positions members of Congress are allowed access to classified information. However, staffs of members and committees must have an appropriate security clearance prior to gaining access to classified information. Security clearances of Congressional staff must be verified through the operating unit's servicing security officer and forwarded to the Office of Security.

3. Individuals who release classified information shall assure that the designated security classification is still valid and that the recipient is advised of the need to protect the information from unauthorized disclosure.

B. General Accounting Office. Properly cleared and identified representatives of the General Accounting

Office (GAO) can be granted access to classified information originated by the Department when the information is relevant to an ongoing GAO review or investigation. The security clearance of a GAO official shall be verified through the Office of Security prior to release of the classified information.

C. Judiciary.

1. An employee, office, or operating unit receiving an order or subpoena issued by a Federal or state court of record to produce classified information shall immediately refer the order or subpoena to the appropriate General Counsel's office. Classified information shall be subjected to an "in camera" review by the judge of the court of record to determine the relevancy of the information in question.

2. If classified information is to be introduced as evidence, access must be limited to the presiding judge of the court and the attorneys and other persons whose duties require knowledge or possession of the information and who have been cleared in accordance with applicable regulations. Additionally, the following safeguards must be followed.

a. All proceedings must be held in a secure court or hearing room.

b. Dissemination and accountability controls must be established for all classified information marked for identification or offered or introduced as evidence.

c. The transcript of the proceeding must be properly marked to indicate the classified portions that must be segregated from unclassified portions and properly safeguarded and stored.

d. Any classified notes, drafts, or other documents produced by non-Commerce individuals, no longer required by any party to the proceeding, must be transferred to the Department for destruction.

e. Each recipient of classified information disclosed under the provisions of Section III, National Security Information, shall be advised of the classification level, safeguard and storage requirements, and the liability in the event of unauthorized disclosure.

f. At the conclusion of the proceeding, all classified information shall be returned to the Department or placed under seal of the court of record.

g. Classified information shall not be introduced as evidence at a civil trial before a jury.

D. Industrial, Educational, and Commercial Entities. Certain bidders, contractors, grantees, educational, scientific, or industrial organizations shall receive classified information only under the procedures prescribed by the National Industrial Security Program (see Chapter 43, Industrial Security).

2110 Dissemination Outside the Federal Government

A. Classified information under the control of the Department shall be released outside the Federal Government to organizations such as state or municipal agencies, firms, corporations, educational institutions, private individuals, or other non-federal sources provided the recipient:

1. Is acting in a contractual or official capacity with the Department; and

2. Has a need-to-know the information to further the mission of the Department.

B. In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the Director for Security may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with the directives implementing E.O. 12958 and procedures described in the Security Manual governing the release of classified information. The disclosure of classified information under these circumstances and the number of individual authorized access shall be minimized consistent with operational necessity. Information disclosed under this provision shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information.

C. The employee releasing the information must verify the recipient's security clearance and facility clearance through the operating unit's security contact.

D. Any proposed releases of classified information outside the Department not specifically covered by this chapter shall be coordinated with the Office of Security before release.

2111 Dissemination of Restricted and Formerly Restricted Data

Information bearing the warning notices, **"Restricted Data"** or **"Formally Restricted Data"** shall not be disseminated outside the Department without the consent of the originator. The originator of the **"Restricted Data"** or **"Formally Restricted Data"** is the Department of Energy (see E.O. 12958).