



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

Chapter 12 - Access to National Security Information

1201 Granting Access to Classified Information

This chapter covers investigative processing procedures and requirements associated with granting eligibility for access to classified national security information, also known as a security clearance. The granting of eligibility for access to classified information is an administrative decision and is used only when access is clearly consistent with the interests of national security. Access to classified information is based on an appropriate background investigation, a security indoctrination, an executed nondisclosure agreement, and a need-to-know. The Director for Security may grant a security clearance upon determination that the individual is trustworthy and free from unacceptable risk concerning the protection of classified information. Security clearances within the Department are issued at the Top Secret and Secret levels. Individuals requiring access to Confidential information will be granted a clearance at the Secret level. The need-to-know is established by management officials based upon the official duties of the position that the employee occupies.

A. Eligibility for Access to Classified Information.

1. A security clearance is an indication that a decision of trustworthiness has been made and has been granted by the Director for Security in accordance with E.O. 12968, Access to Classified Information. A need for access to classified information must be demonstrated before a request for a security clearance can be initiated. The number of people cleared and granted access to classified information should be maintained at the minimum number that is consistent with operational requirements and needs. Heads of operating units must ensure that access to classified information by unauthorized persons is prevented.

2. No one has a right to gain access to classified information solely by virtue of title, position, or level of security clearance. The final responsibility for determining whether an individual requires access to classified information and whether the individual has been granted the appropriate security clearance rests upon the individual who has possession, knowledge, or control of the information and not upon the prospective recipient. The fact that an individual is a Federal employee does not mean that he or she has been cleared for access to classified information. The disclosure of classified information and the recipient's identification and security clearance shall be verified by the security contact to determine the recipient's need-to-know. The individual holding or controlling classified information shall advise the recipient of the classification level of the information.



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

3. Accordingly, when an employee transfers or vacates a position, his need-to-know changes. Security clearances do not transfer with the employee. In such cases, the need-to-know must be re-established and a new request submitted to their servicing security officer with appropriate justification before a new clearance is granted. Depending on circumstances, the existing investigation may be used as the basis for issuing the new clearance.

B. Determining Eligibility for Access to Classified Information.

The procedures for requesting personnel security investigations for sensitive positions are listed in Appendix D, Processing Personnel Security and Suitability Investigations, paragraph D.3, Processing Investigations. Requests for upgrade or reinstatement of a security clearance also are covered in paragraph D.3 of Appendix D.

1. A person's eligibility for a security clearance and access to classified information are based upon the following criteria.

a. **Eligibility:** The individual is found loyal, trustworthy, and free from unacceptable risks, based upon an appropriate investigation.

b. **Access:** The access to classified information is essential to accomplish a lawful and authorized government purpose (need-to-know) and the individual has entered into an agreement with the Federal Government to protect classified information and to prevent unauthorized disclosure. The Classified Information Nondisclosure Agreement, Standard Form 312, shall be used for employees and non-employees.

2. The decision to grant eligibility for access to classified information must be fair, impartial, and based upon a consideration of all available information. The review of adverse information shall include consideration of the following factors.

a. Nature and seriousness of the facts, circumstances, or conduct.

b. Circumstances surrounding the conduct.

c. Frequency and recency of the conduct.

d. Age of the individual.



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

- e. Motivation of the individual, or the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the circumstances or consequences involved.
 - f. Absence or presence of positive evidence of rehabilitation.
 - g. Probability that the facts, conduct, or circumstances, to the extent that it can be estimated, will or will not continue or recur in the future.
3. National security and suitability investigations described in Chapter 11 are also used for making security clearance determinations. The type of investigation needed to provide a basis for a security clearance determination is provided in Appendix C, Minimum Requirements for Personnel Investigations.
4. The following general requirements apply to the process of determining eligibility for access to classified security information.
- a. Naturalized citizens may be considered for access eligibility in the same manner as native-born U.S. citizens.
 - b. Foreign nationals generally are not eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to an immigrant alien or a foreign national. Such individuals may be granted a Limited Access Authorization in those rare circumstances where the non-U.S. citizen possesses unique or unusual skill or expertise that is urgently needed to support a specific U.S. Government contract involving access to specified classified information and a cleared or clearable U.S. citizen is not readily available (see NISPOM, Section 2-210, Non-U.S. Citizens).
 - c. Contractors may be granted a security clearance under the National Industrial Security Program. Refer to Chapter 43 of the Security Manual concerning Industrial Security. On a case-by-case basis, the Office of Security may grant individual contractors a security clearance for the performance of short-term classified work. Information on processing this request is contained Appendix E, Obtaining Access to Classified Information.
 - d. Non-employees other than contractors generally will not be provided access to classified information. Some exceptions exist for those non-employees being processed for membership on a departmental advisory committee, which requires access to classified information.



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

C. Exceptions. Within the limits of administrative discretion permitted to the Department, exceptions to the provisions of this subparagraph may be granted by the Director for Security, or his/her designated representative whenever such an exception would be in the interest of the national security and would promote the efficiency of the service. Each request for such an exception shall be submitted in writing and shall contain a statement justifying the request.

1202 Requesting a Security Clearance

A. Request Forms. The immediate supervisor or program manager must request and justify a security clearance for a subordinate employee. The request must be forwarded to the Office of Security through the servicing security officer. The Form CD-79, Request for Security Clearance, shall be used to request a security clearance. In addition, the SF-86, Questionnaire for National Security Positions, is required. Incomplete packages will be returned through the security contact or servicing security officer to the operating unit for appropriate action.

1. The CD-79 must state the level of clearance (Top Secret or Secret) and must justify the request for access. The request must describe the individual's "need-to-know," the nature of access, how often it will occur, and the duration required for the clearance. If the duration is indefinite, it must be so stated. The security contact must concur by signing the concurrence block on the CD-79.
2. The SF-86 provides current biographical information to establish eligibility for access. A new or an updated SF-86 is required when the Office of Security does not have one on file.
3. Note: The SF-312 can be signed only after eligibility for access to classified information has been granted by the approving authority; therefore, it will not be sent in the clearance request package. The individual must sign the form immediately after receiving the indoctrination briefing since it is a legally binding document that grants the signer eligibility for access to classified information upon signature in return for abiding by its requirements. The supervisor or manager requesting a security clearance for a subordinate employee should follow the procedure described in Appendix E, Obtaining Access to Classified Information.

B. Temporary Eligibility for Access.

1. Based on a justified need meeting the requirements of E.O. 12968, temporary eligibility for access to classified information may be granted before investigations are complete and favorably adjudicated where official functions must be performed prior to completion of the investigation and adjudication process. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the



U.S. DEPARTMENT OF COMMERCE MANUAL OF SECURITY POLICIES AND PROCEDURES

Department may revoke the access at any time based on unfavorable information developed in the course of the investigation.

2. Temporary eligibility for access must be requested by memorandum to the Office of Security. In addition, the justification for the access must be indicated on the CD-79, Request for Security Clearance. The Director for Security, or his/her designee, may grant temporary eligibility for access when an emergency need exists. Temporary eligibility allows access to classified information under controlled circumstances when the basis for granting a final security clearance has not been completed.

1203 Administrative Downgrade or Termination of Security Clearance

A. A security clearance may be downgraded or terminated for administrative reasons unrelated to an adverse security determination. Just as the immediate supervisor or program manager is responsible for requesting a security clearance, he or she also is responsible for advising the Office of Security, through the security contact or the servicing security officer, whenever administrative downgrade or termination of security clearance is appropriate based on changed need-to-know. Whenever there is an administrative action, the individual must be advised of the action. The administrative downgrade or termination of an individual's security clearance does not prejudice the person's eligibility for a future security clearance. Administrative action is required in the examples noted below. In each case of termination or downgrade of access to national security information, the servicing security officer shall notify the servicing human resources management office so that the position records may be updated.

1. When access to classified information is no longer needed in connection with the performance of official duties or contractual obligations, the clearance must be withdrawn. In such cases, the immediate supervisor or manager must obtain a signed SF-312 with the debriefing portion completed and forward it through the security contact or the servicing security officer to the Office of Security headquarters.

2. When access to a particular level of classified information is no longer required in the performance of official duties, the clearance must be downgraded to a classification level still justified by official duties. To initiate a downgrade action, the immediate supervisor must forward a CD-79, Request for Security Clearance, justifying the new clearance level indicating, "Administrative Downgrade," in the "Justification Block" of the form, and stating that the employee has been notified of the downgrade action.

3. An operating unit head or designee, or the Director for Security may determine that a currently cleared employee or contractor no longer requires access to classified information in connection with the performance of official duties or contractual obligations and, upon written notification to the holder, may administratively withdraw the security clearance. When an individual no longer needs access to a



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

particular security classification level, the security clearance should be adjusted, or downgraded, to the classification level required for the performance of the individual's duties and obligations.

4. Upon termination of a security clearance, the holder must 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 SF-312, Classified Non-Disclosure Agreement, shall be completed upon debriefing. In addition, sanctions under Title 18, U.S.C. shall be provided in writing to the debriefed employee to re-emphasize that criminal prosecution may be exercised if unauthorized disclosure of classified information should occur.

B. Classified information (in any form), to include extra copies, is not personal property and may not be removed from the Federal Government's control by any departing official. The security contact must ensure that all debriefed personnel have turned over all classified information in their possession and ensure that all classified information is accounted for upon transference to an authorized custodian. All departing personnel must be debriefed and understand their ongoing security responsibilities in the protection of classified information to which they had access.

1204 Suspension and Revocation of Access Eligibility for Cause

A. Whenever information is received that indicates an employee's continued access to classified information is not in the interests of national security, such information shall be forwarded immediately to the Office of Security headquarters. Guidelines for standards of conduct related to security determinations are set forth in Chapter 13, Security Adjudication Criteria.

B. Whenever the Personnel Security Officer obtains information that suggests continuation of an individual's security clearance is not in the best interest of national security, he or she may suspend the individual's security clearance pending an investigation to resolve the issues.

C. Accordingly, whenever an investigation develops information that confirms an individual's disloyalty to the country or untrustworthiness, or raises issues of unacceptable security risk, the Personnel Security Officer will issue a proposal to revoke or downgrade an individual's security clearance, as appropriate. Such security determinations for cause will be made independently of a suitability determination conducted by the servicing human resources manager.

D. The servicing human resources manager and servicing security officer will be advised of all security clearance actions for cause. When an individual's security clearance has been suspended, the servicing security officer must notify the immediate supervisor or program manager to ensure that appropriate action is



U.S. DEPARTMENT OF COMMERCE MANUAL OF SECURITY POLICIES AND PROCEDURES

taken in connection with the individual's access to classified information.

E. The procedures described in Chapter 14, Suspension and Revocation of Access to National Security Information, shall be followed by the Office of Security when conducting a formal review to determine an individual's continued eligibility for access to classified information based on unfavorable information that may lead to the denial, downgrade, or revocation of that clearance.

1. When misconduct is reported to the servicing human resources office and the individual occupies a sensitive position, the servicing human resources specialist shall contact the servicing security officer immediately. The investigation of the misconduct must be coordinated, and normally, the national security interest will be investigated first.

2. The results of the investigations are shared between security and human resources offices. The Office of General Counsel should be included in the deliberative process to decide what action(s) to take.

1205 Access to Classified Information for Employees

Employees of the Department (including experts and consultants) who are U.S. citizens may be considered for access to classified information only when such access is required in connection with their official duties. Such individuals may be granted either a final or a temporary eligibility for access to classified information provided that the appropriate investigative requirements set forth in the Security Manual are met, all available information has been favorably adjudicated, and the granting of eligibility for access to classified information is clearly consistent with national security interests. Criteria for determining eligibility of access to classified information are shown in paragraph 1201 B.

A. Investigative Requests and Procedures. Procedures for the various types of investigations listed below are described in Appendix E.

1. Although position sensitivity may dictate a more detailed investigation, the following security clearance levels require the minimum type of investigation as indicated below.

a. **Top Secret:** an SSBI no more than five years old, or updated by an SSBI-PR within the most recent five-year period.

b. **Secret:** an ANACI no more than ten years old and continuous Federal service.

2. Prior to movement to a new position which requires access to classified information or when the



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

assignment results in a significant change in duties, a request for security clearance (CD-79) must be forwarded through the servicing security officer to the Office of Security for approval, even if the assignment involves the same level of security clearance as the employee's current position.

3. When an employee occupies a position that subsequently requires access to classified information, the employee may continue to perform in the position provided that access to classified information is prevented until the Office of Security grants an appropriate security clearance.

4. When an employee moves to a position that requires access to a higher level of classified information, the employee may continue to perform in the position and may continue to have access to classified information at the level for which he or she has previously been granted until the Office of Security upgrades the security clearance to the higher level clearance or grants the appropriate level of temporary access.

5. In the event that a foreign national employee who does not meet the criteria listed in paragraph 1201B requires access to classified material on a short-term, emergency basis, a request for such access, in addition to forms required under paragraph 1202, shall be forwarded through the security contact or servicing security officer to the Office of Security. The request should state the specific reasons for the required access, justify the individual's "need-to-know," provide detailed provisions to ensure that access to classified information is limited to "need-to-know," and indicate the expected duration of the requirement.

B. Certification of Security Clearance. Any employee, contractor, or consultant of the Department who has a need to certify their security clearance for a visit to another agency or facility, must initiate the Visit Authorization and Clearance Certificate Request, Form CD-414. The form must be completed, signed by the approving security contact or servicing security officer, and submitted to the agency or facility to be visited. The form shall be submitted as soon as possible as the visit is determined, or at a minimum, within ten working days of the visit or the period of clearance certification. There are other agencies or government facilities that do not accept the Department's CD-414, but require use of their own form for visits to their facilities. The method acceptable to the visited agency should be verified in advance by the individual coordinating the visit.

1206 Access to Classified Information for Non-Employees

The assignment of non-employees to positions requiring access to classified information is discouraged with the exception of essential contractors, experts and consultants, and advisor committee members. The assignment of foreign national non-employees to activities requiring access to classified information, or which may involve incidental access to classified information, is strictly prohibited.



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

A. Investigative Requests and Procedures. Non-employees who interact with the Department include, but are not limited to, contractors, research associates, guest workers, trainees, members of advisory committees, historical researchers, former presidential appointees, and visitors. Information and procedures on obtaining security clearances for consultants and experts are included in the coverage for non-employees in paragraph 1104. Information on obtaining security clearances for all non-employees is included in Appendix E, Obtaining Access to Classified Information.

1. **Contractors** working on classified contracts are required to obtain an appropriate security clearance in accordance with the National Industrial Security Program (NISP). The program is described in Chapter 44 of the Security Manual. The Office of Security may grant a contract employee eligibility for access to classified information for the performance of short-term classified work. No classified material can be removed from a departmental facility. All classified materials must remain under the Department's absolute control.

2. **Guest Workers, Research Associates, and Trainees** are usually screened for suitability factors by the "security assurance" process described in paragraph 1104. Assignments that require access to classified information are discouraged for these individuals; however, for specific projects or activities, a security clearance may be granted under limited conditions.

3. **Advisory Committee members** will require a security clearance if the committee requires access to classified information. Generally, security clearances for advisory committee members are granted at the Secret level.

4. **Historical Researchers and Former Presidential Appointees** may be cleared by the Director for Security at an appropriate level to allow access to the Department's classified information. Refer to paragraph 1104 for further guidance.

5. **Visitors** to the Department:

a. **Employees, Contractors, or Consultants of another Federal Government** agency may obtain access to classified information in the Department in the performance of official duties under the provisions of Chapter 21, Access and Dissemination, and after the verification of an appropriate security clearance through security channels. In the case of repeated short-term visits by such an individual, clearance certification must be provided at least annually from the Federal agency concerned to the servicing security officer.



**U.S. DEPARTMENT OF COMMERCE
MANUAL OF SECURITY
POLICIES AND PROCEDURES**

b. *Private Citizens* who have not been granted a security clearance and who have no need-to-know are prohibited access to classified information, areas, or equipment.

6. Before a non-employee may be granted access to classified information sponsored by another Federal agency, the security contact or servicing security officer shall obtain approval from the sponsoring agency (see paragraph 1104). When such a project is carried out under the security regulations of the sponsoring agency, the personnel security requirements of the sponsoring agency apply.

B. Exceptions. Subject to such policies and directives as the Chief Financial Officer and Assistant Secretary for Administration may prescribe, exceptions to the provisions of this chapter may be granted in unusual cases by the Director for Security whenever the facts indicate that such an exception is in the national interest. Each request for such an exception must be made in advance, in writing, and be submitted to the Director for Security. The request must contain a detailed justification for the exception.