Chapter 5 - Security Inspections and Assistance

501 Purpose

A. Departmental of Commerce security policy is designed to ensure proper and adequate security services to customers while safeguarding and protecting all departmental assets and interests from theft, sabotage, and/or hostile acts. Threats to the Department have an adverse impact on national security and threaten the health and safety of the Department's employees, contractors, other individuals, and the public. Security inspections, which may consist of security surveys, assessments, assistance visits, compliance reviews, and unannounced spot checks, are conducted to ensure compliance with laws, Executives Orders, Federal regulations, and departmental policies.

B. This chapter provides an overview of security inspections conducted by the Office of Security and sets standards for establishing and maintaining an ongoing self-inspection program in the operating units. Departmental policy mandates that security inspection programs shall include the periodic internal review and evaluation of individual operating unit activities with respect to the effective implementation of the classified National Security Information Program as established under the E.O. 12958, Classified National Security Information. These standards are binding and apply to all offices that process, handle, and/or store classified information, equipment, or materials, including contractors and Federal advisory committee members, pursuant to the National Industrial Security Program described in E.O. 12829.

C. The National Industrial Security Program Operating Manual (NISPOM) prescribes the security requirements, restrictions, and safeguards applicable to private industry under U.S. Government contract, including contractor conducted self-inspections. The standards established in the NISPOM are consistent with the standards prescribed E.O. 12958.

D. The Director for Security is responsible for ensuring that all departmental operating units comply with established security laws, regulations, and policies. Compliance review teams, which conduct compliance surveys, inspections, assessments, and spot checks, carry out this function.

502 Inspection Procedures and Frequency of Compliance Reviews

A. Inspection procedures and frequency of compliance reviews are based on program needs and the magnitude of security activity. Activities that process classified information shall conduct at least one internal classified document review per year. Servicing security officers will ensure that

classified storage containers within their respective areas are inspected annually. Compliance review teams will conduct classified national security oversight inspections of operating units biannually and shall coordinate these inspections with the respective servicing security offices. Security inspection teams will develop and present an inspection summary, then provide the summary and an outbriefing to the inspected activity or operating unit on the final day of the inspection.

B. Compliance review teams will prepare a draft report that documents the findings and recommendations of each inspection and forward it to the appropriate operating unit official. Copies of biannual reports will be sent to the servicing security officer and responsible security contact. The Office of Security will determine the need for follow-up validation visits or inspections to ensure corrective action has been taken on findings involving discrepancies noted during the initial inspection.

C. The elements of the security inspection program include, but are not limited to, the elements noted in the following paragraphs. The scope of the self-inspection may expand according to program and policy needs. Each inspection of an operating unit's security program need not include all the elements covered below. Means and methods for conducting inspections may include:

1. A review of relevant security directives, guides, and instructions;

2. Interviews with key personnel, classifiers, users, and/or holders of classified materials;

3. A review of access and control records;

4. A review of internal procedures and processes pertaining to the protection, control, and safeguarding of classified and sensitive information; and

5. A review of a sampling of Secret-level materials and/or a review of all Top Secret materials processed and/or stored by the operating unit activities.

503 Coverage of Compliance Inspections

Compliance review teams will review the security policies and procedures carried out in the various operating units to determine compliance with the Department's security programs. Elements of the security inspection program are indicated in the section noted below, but are not limited to these items. Each compliance review of a classification activity need not include all the elements covered below.

A. Original Classification.

1.The review team will evaluate an Original Classifying Authority's (OCA) general understanding of the process of original classification, to include:

a. Applicable standards for classification;

b. Levels of classification and the damage criteria associated with each; and

c. Required classification markings.

2. The review will determine if delegations of original classification authority conform to the requirements of E.O. 12958, to include whether:

a. Delegations are limited to the minimum number necessary to effectively administer the program;

b. Designated original classifiers have a demonstrable and continuing need to exercise this authority;

c. Delegations are in writing and identify the official by name and position title; and

d. All requests for delegation of classification authority are justified and approved in writing by the Secretary of Commerce.

3. The review will assess the OCA's familiarity with the duration of classification requirements, to include:

a. Assigning a specific date or event for declassification when possible;

b. Establishing a maximum 10-year duration of classification when an earlier date or event cannot be determined;

c. Limiting extensions of classification for specific information for successive periods not to exceed ten years at a time; and

d. Exempting specific information from declassification within ten years, as provided in Section 1.6 of E.O. 12958.

4. A review will be conducted of a random sampling of classified information generated by the inspected activity to determine the application of proper and complete markings.

5. The review team will evaluate the OCA's classification actions to determine if they comply with the standards specified in paragraphs 1803 and 1905 of the Security Manual, as related to classification and declassification guides, respectively.

6. The review will verify that OCA classification actions do not violate the prohibitions and limitations on classification.

7. The review will assess whether the OCA's procedures to challenge classification decisions meet the requirements of the E.O. 12958 and the Security Manual.

B. Management and Oversight. Prior to making original classification decisions, the original classification authority must be trained on the proper procedures for such actions. The Compliance Review teams will assess whether:

1. Appropriate training was provided to an OCA;

2. Senior management demonstrates an active commitment to the overall success of the security program, to include providing the necessary resources for effective implementation and policy compliance;

3. Users and holders of classified information receive guidance concerning security responsibilities and requirements;

4. Effective controls are established and maintained to prevent unauthorized access to classified information;

5. Contingency plans are established and understood by all personnel responsible for safeguarding classified information during emergencies or disasters;

6. The performance rating system used to rate employees on job performance includes the management of classified information as a critical element or item to be evaluated in the rating of original classification authorities, security managers or officers, security specialists, classification management officers, classified control points, and other employees involved with the storing, processing, or handling classified information; and

7. A defined system is in place for collecting information on the estimated costs associated with the implementation of E.O. 12958 for classification and declassification related activities. This system shall be established and implemented by the servicing security officer in coordination with original classification authorities.

C. Derivative Classification. The compliance review teams will assess the general familiarity of individuals who perform derivative classification actions to determine their understanding of

the following requirements:

1. Conditions for derivative classification;

2. Requirement to consult with the originator of the information when questions concerning classification arise;

3. Proper use of classification guides; and

4. Proper and complete application of classification markings to derivatively classified documents. Derivative documents must carry forward all markings (to include portion markings) and declassification instructions.

D. Declassification. The compliance review teams will inspect the following declassification actions and activities.

1. The team will verify whether the operating unit/OCA has established, to the extent practical, a system of records management to facilitate public release of declassified documents.

2. The team will evaluate the status of the operating unit/OCA's declassification program, including the requirements to:

a. Comply with the automatic declassification provisions regarding historically valuable records over 25 years old;

b. Declassify, when possible, historically valuable records prior to accession into the National Archives;

c. Provide the Archivist with adequate and current declassification guides;

d. Ascertain that the mandatory review program conforms to established requirements; and

e. Determine whether responsible agency officials are cooperating with the Archivist in the development and maintenance of a Government-wide database of information that has been declassified.

E. Safeguarding. The compliance review teams will review an operating unit's national security information program to determine compliance with the following items:

1. Adherence to established standards for safeguarding classified and sensitive information;

2. Compliance with controls for access to classified information;

3. The effectiveness of the information security program in detecting and processing security violations and preventing recurrences;

4. Assess compliance with the procedures for identifying, reporting, and processing unauthorized disclosures of classified information; and

5. Evaluate the effectiveness of procedures to ensure that:

a. The operating unit exercises proper control over the classified information it generates, processes, handles and/or stores;

b. Holders of classified information do not disclose information originated by another agency without that agency's authorization; and

c. Departing or transferring individuals with access to classified information return all classified information in their possession to their designated classified control point or other authorized, cleared agency personnel prior to termination of security clearance.

F. Security Education and Awareness Program. The compliance review team will evaluate the effectiveness of the servicing security officer's security education and awareness training program in familiarizing and refreshing appropriately cleared personnel with regulations, policies, and procedures concerning National Security Information. The review will also determine whether the program meets the standards specified in paragraph 301 of the Security Manual.

504 Self Inspection

Servicing security officers and security contacts will periodically conduct inspections in their operating unit or units to review compliance with the Department’s security policies and procedures. The scope of these inspections may vary according to program needs. The frequency of the inspection in each unit will be determined by the servicing security officer or the security contact.