Department of Homeland Security
Management Directive System
MD Number: 11035
Issue Date: 02/10/2005

INDUSTRIAL SECURITY PROGRAM

I. Purpose

This directive establishes the Industrial Security Program for the Department of Homeland Security (DHS).

II. Scope

This directive applies to Department of Homeland Security (DHS) Headquarters and all Organizational Elements within DHS. The provisions of this directive are established to ensure that U.S. industry partners performing work for DHS as contractors, subcontractors, consultants, licensees, and grantees, and involving access to classified information, comply with the standards for safeguarding such information pursuant to the National Industrial Security Program (NISP).

This directive also applies to firms and/or individuals performing under contract to DHS from pre-contract award to post-contract completion.

III. Authority

A. Executive Order 12958, as amended, “Classified National Security Information,” dated March 28, 2003.

B. Executive Order 12829, “National Industrial Security Program,” dated January 6, 1993.

C. Department of Defense (DOD) Manual 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM) for Safeguarding Classified Information,” with supplements, dated February 2001.

D. Memorandum from the Secretary of Homeland Security, “Designation of Senior Agency Official,” dated March 3, 2004.

E. Management Directive 0010.1; "Management Directives System and DHS Announcements."

IV. Definitions

A. ***Carve-Out Contracts***: A classified contract issued in connection with an approved SCI or Special Access Program in which the Defense Security Service has been relieved of inspection responsibility under the Defense Industrial Security Program, in whole or in part.

B. ***Classified Contract***: Any contract that requires, or will require, access to classified information by a contractor or his/her employees in the performance of the contract. A contract may be classified even though the contract document is not classified. The requirements prescribed for a classified contract are also applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Contracting Agency programs, or projects, that require access to classified information by a contractor.

C. ***Classified Visit***: A visit during which the visitor will require, or is expected to require, access to classified information.

D. ***Cognizant Security Agency (CSA)***: Agencies of the Executive Branch that have been authorized, by E.O. 12829, to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry.

E. ***Contractor***: Any industrial, educational, commercial, or other entity that has been granted a facility security clearance by a cognizant security agency (CSA).

F. ***Contract Security Classification Specification (DD Form 254)***: The DD Form 254, with any attachments or incorporated references, is the legally binding exhibit of a federal contract. It is the only authorized vehicle for conveying to a contractor the security classification guidance for classified national security information.

G. ***Facility Clearance***: An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

H. ***Foreign Government***: Any national governing body organized and existing under the laws of any country, other than the United States and its possessions and trust territories, and any agent or instrumentality of that government.

I. ***Organizational Element***: As used in this directive, Organizational Element is as defined in DHS MD Number 0010.1, "Management Directive System and DHS Announcements."

J. ***Personnel Clearance (PCL)***: An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the PCL being granted.

K. ***Senior Agency Official (SAO)***: An official designated by the agency head under section 5.4(d) of E.O. 12958, as amended, who directs and administers the agency's program under which information is classified, safeguarded, and declassified. The Senior Agency Official for DHS is the Chief Security Officer.

V. Responsibilities

A. The Secretary of Homeland Security has designated the Chief Security Officer (CSO) as the Senior Agency Official (SAO). The Senior Agency Official shall direct and administer DHS's industrial security program.

B. The Chief, Administrative Security Division shall administer, manage, and provide oversight for the industrial security program, under the direction and authority of the CSO/SAO.

C. Contracting Officers shall ensure that all solicitations and contracts under their oversight comply with the policies and procedures identified in this directive, in addition to the requirements of the Federal Acquisition Regulation regarding safeguarding classified information.

VI. Policy & Procedures

A. ***Policy***. DHS is a signatory to and participates in the National Industrial Security Program. The NISP was established by Executive Order 12829, on January 6, 1993, to protect information classified pursuant to Executive Order 12958, "Classified National Security Information," as amended, and the Atomic Energy Act of 1954, as amended. The President has designated the Secretary of Defense as Executive Agent for the NISP. The Director, Information Security Oversight Office (ISOO), is responsible for implementing and monitoring the NISP, and for issuing implementing directives that shall be binding on OEs.

1. The NISP was developed to serve as a single, integrated, cohesive program for the protection of classified information when not in U.S. Government possession. Under the NISP, contractors are mandated to protect all classified information to which they have been given access or custody by U.S. Government Executive Branch departments or agencies.

2. DHS formalized its use of the industrial security services of the Department of Defense, as a user agency of the NISP, by Memorandum of Agreement dated August 22, 2003. As a result of the agreement, the

DOD is authorized to act for and on behalf of DHS in rendering security services for the protection of classified information released to or within industry by DHS. DHS participates in the NISP to ensure that any classified information released to or accessed by industry, in connection with DHS contracts, grants, or related activities, is properly safeguarded in accordance with Executive Order 12958, as amended.

3. Participation in the NISP allows DHS to use the Defense Security Service (DSS) to conduct investigations for contractor facility and personnel security clearances, and to monitor the contractor's compliance with safeguarding requirements. All facility and personnel security clearances granted by DOD will be accepted by DHS to establish eligibility for access to classified information. Contractors granted an interim facility and personnel clearance, such as an interim TOP SECRET, will only be eligible for access to DHS classified information at the SECRET level. Upon completion by DSS of all investigative requirements, that facility shall be considered eligible for access to classified information, or contract award, at the appropriate level granted by DSS.

4. DSS issues and maintains facility security clearances and personnel security clearances, as required, for DHS contractors. DSS inspects and monitors contractors who require or will require access to classified information. The Defense Industrial Security Clearance Office (DISCO), a field element of DSS, issues personnel security clearances under the authority of the NISP.

B. ***Procedures***.

1. National Industrial Security Program Operating Manual (NISPOM). The NISPOM (DOD 5220.22M) gives practical application to the objectives of the NISP (Executive Order 12829) by serving as the single regulatory standard for the NISP. The NISPOM prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information, and to control authorized disclosure of classified information released by U.S. Government Executive Branch departments and agencies to their contractors, in accordance with the NISP. The NISPOM also prescribes requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program information.

2. Program Management. Department and Organizational Element programs, projects, and contracting personnel must consider security requirements at the earliest possible stage in the procurement process.

The responsibility for effective implementation of DHS's Industrial Security Program must be shared by the project manager, contracting officer's technical representative/contracting officer's representative, security officials, the contracting officer, and the contractor.

3. Security Clearances. To ensure that classified information entrusted to private industry is properly safeguarded, DHS requires that contractors who will require access to classified information in the completion of their contractual responsibilities, be processed for security clearances in accordance with the requirements stipulated in the NISPOM.

4. Facility Security Clearance (FCL).

a. Any firm or business under contract with DHS, which requires access to classified information, will require a facility security clearance commensurate with the level of access required. Additionally, any firm or business entity that requires access to classified information to prepare a response to a Request for Proposal, Request for Bid, etc., and/or in performance of a classified Department contract, will require a facility clearance.

b. Firms that do not possess a facility clearance, or the requisite level of facility clearance, will be sponsored for a DOD facility clearance when a determination has been made by the government contracting officer that the contract effort will require access to classified information. Facility clearance sponsorship requests will be made by the respective Organizational Element directly to the DSS. Organizational Elements that do not have an Industrial Security Program shall submit sponsorship requests to the DHS Office of Security, Administrative Security Division (ASD). DHS ASD will process such requests to DSS.

c. Facility clearances for sub-contracts shall be sponsored and processed by the prime contract in accordance with the NISPOM.

5. Contractor Personnel. Individuals employed by a contractor will be cleared through DISCO. The cleared contractor is required to have a designated facility security officer (FSO) through whom requests for personnel security clearances are submitted to DISCO. The FSO will provide the appropriate DHS security office and contracting office with an updated status report of security clearance actions requested, pending, and approved as required. The FSO is also responsible for submitting visitor authorization requests on all cleared employees. Contractor personnel must have clearances commensurate with the level of access required for performance under the contract. DHS has no role in the processing or granting of security clearances to industry personnel.

6. Contract Security Classification Specification (DD Form 254).

a. In order to activate DSS services and obligate the contractor to the provisions of the NISPOM, Organizational Elements will include, in all classified contracts and classified contract solicitations, a “Contract Security Classification Specification” (DD Form 254). This DD Form 254 is the primary vehicle for relating contract specific security classification guidance to the contractor and shall, therefore, in Section 13 of the form, prescribe the source(s) from which the contractor shall derive classification requirements. The source(s) shall either identify a published Security Classification Guide(s) applicable to the contract effort, or that classification will be based on existing classified information from which the contractor shall derive and apply classification guidance. Where the source(s) is identified as a security classification guide(s), the contractor shall be provided access to, or a copy of, the applicable guide(s).

b. A DD Form 254 is required and will be completed only for contracts that require access to classified information.

c. Organizational Elements that have an established Industrial Security Program shall prepare and process a DD Form 254 for each classified contract. A copy of all completed DD Forms 254 issued by Organizational Elements shall be submitted to DHS/ASD.

d. Organizational Elements that do not have an established Industrial Security Program will coordinate preparation of the DD Form 254 with DHS/ASD. The statement of work or other documentation used to describe the services or supplies that will be provided by the contract will be provided to DHS/ASD to assist in preparing the DD Form 254.

e. The contract, statement of work, or other documentation shall contain a security clause that a Government contracting officer made a determination that the contract issued will require access to classified information by the contractor or his or her employees in the performance of the contract. This requirement shall be prescribed for all DHS classified contracts, and will be applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Contracting Activity Programs that require access to classified information by a contractor.

f. In those cases where DHS/ASD prepares the DD Form 254, they will return the approved DD Form 254 to the Organizational Element for inclusion in the contract or solicitation. DHS/ASD will distribute a copy of the DD Form 254 to DSS, the contractor, and other OEs as applicable. DSS will conduct investigations and issue the personnel security clearance(s) for the contract employees. With the exception of "carve out" contracts requiring access to Sensitive Compartmented Information or other Special Access Programs (SAPs), DSS will provide security oversight functions in coordination with the Contractor's Security Officer. DHS, Office of Security, Special Security Programs Division will provide oversight for contracts involving access to SCI and SAP information.

g. In some instances it may be necessary to include classified information in a DD Form 254 and facility clearance request. In these cases, the documentation must be protected in a manner approved for classified information.

7. Classified Visits

a. Visit Requests. Organizational Elements are to accept visit authorization letters only when they are submitted in accordance with, and contain the information as required by, Chapter 6 of the NISPOM.

b. Approvals.

(1) All classified visits by contractors require advance notification to the Organizational Element hosting the visit.

(2) Organizational Elements will only accept visit requests in writing. The visit authorization letter may be submitted either by mail, facsimile, or teletype, in sufficient time to allow for approval or disapproval of the requested visit. Telephonic verification of a visit request shall not be accepted except under unique circumstances where: the failure to provide immediate access will have an adverse impact on the mission; unusual circumstances prevented the receipt or transmission of a written visit request; there is a means to authenticate the validity of the telephone request; and acceptance of telephonic verification is approved by program management personnel. Instances not meeting this criteria shall result in a delay or denial of access until such time as a written request is received. Where telephonic verification is approved, written confirmation shall immediately follow.

(3) Hand-carried visit requests shall not be accepted.

(4) The Organizational Element having security cognizance has final approval authority for the proposed visit. Organizational Elements need not notify a requester that a visit has been approved if sufficient advance notice of the visit was provided. If the Organizational Element disapproves a visit, the requester must be promptly notified.

(5) The number of classified visits shall be held to a minimum. The Organizational Element must determine that the visit is necessary and requires access to classified information in order to approve a classified visit.

c. Precautions.

(1) Organizational Elements are to ensure visitors do not take notes, make records of classified discussions, discuss classified information on non-secure telephones, or take photographs in areas where classified information might be recorded, unless given permission by the host Organizational Element, or as otherwise specified in a classified contract.

(2) Organizational Elements are to ensure that access to classified information, higher than the level of the visitor's clearance certified in the visit authorization letter, is not granted. Access shall not be granted if the level of classified information exceeds the level required by a contract or specific purpose identified in the visit authorization letter.

8. International Security Agreement.

a. International Security Agreements with foreign governments address security controls, protection, and assurances for safeguarding classified information. These agreements establish the "government-to-government" principle, signifying that signatory governments each have legal responsibility over the others' classified information at all times. All agreements will be in accordance with Chapter 10 of the NISPOM.

b. DHS/ASD shall be responsible for the administration and oversight of classified material to be exported, the permanent and temporary import of classified information, and compliance by cleared U.S. contractors involved with NATO, foreign governments,

and foreign contractors.

c. DHS/ASD is responsible for maintaining a record of cleared U.S. contractors involved with foreign entities and related activities. Any disclosure or transfer of technical data to a foreign national is considered an “export,” regardless of where the transfer takes place. OEs and contractors desiring to enter into international agreements such as: Visits, Assignments, and Exchanges with Foreign Nationals, will report their intentions to DHS/ASD. The report shall contain:

(1) Name of Country.

(2) Name and address of government entity issuing contract.

(3) Contract/RFP number.

(4) Name of U.S. contractor/name of any subcontractors involved.

(5) Contract/RFP issue and response date.

d. Contractors are still required to report their activities to DSS per the NISPOM.

e. DHS/ASD shall use this report received from contractors to issue proper guidance to the Organizational Elements and to contractors to ensure compliance with governing export control laws, before executing any agreement with a foreign interest that involves access to DHS classified information by a foreign national. Contractors are still required to comply with foreign ownership, control, or influence requirements per the NISPOM. Prior to the execution of such agreements, review and approval are required by the State Department and release of the classified information must be approved by DHS. Failure to comply with Federal licensing requirements may render a contractor ineligible for a facility clearance.

VII. Questions

Any questions or concerns regarding this Directive should be addressed to the DHS Office of Security, Administrative Security Division (DHS/ASD).