

§ 2004.10

transfer; Restricted Data; Special Access Program; or Sensitive Compartmented Information.

[71 FR 18007, Apr. 10, 2006. Redesignated and amended at 75 FR 17306, Apr. 6, 2010]

§ 2004.10 Responsibilities of the Director, Information Security Oversight Office (ISOO) [102(b)].¹

The Director ISOO shall:

- (a) Implement EO 12829, as amended.
- (b) Ensure that the NISP is operated as a single, integrated program across the Executive Branch of the Federal Government; i.e., that the Executive Branch departments and agencies adhere to NISP principles.
- (c) Ensure that each contractor's implementation of the NISP is overseen by a single Cognizant Security Authority (CSA), based on a preponderance of classified contracts per agreement by the CSAs.
- (d) Ensure that all Executive Branch departments and agencies that contract for classified work have included the Security Requirements clause, 52.204-2, from the Federal Acquisition Regulation (FAR), or an equivalent clause, in such contract.
- (e) Ensure that those Executive Branch departments and agencies for which the Department of Defense (DoD) serves as the CSA have entered into agreements with the DoD that establish the terms of the Secretary's responsibilities on behalf of those agency heads.

§ 2004.11 Agency Implementing Regulations, Internal Rules, or Guidelines [102(b)(3)].

(a) *Reviews and Updates.* All implementing regulations, internal rules, or guidelines that pertain to the NISP shall be reviewed and updated by the originating agency, as circumstances require. If a change in national policy necessitates a change in agency implementing regulations, internal rules, or guidelines that pertain to the NISP, the agency shall promptly issue revisions.

(b) *Reviews by ISOO.* The Director, ISOO, shall review agency imple-

¹Bracketed references pertain to related sections of Executive Order 12829, as amended by E.O. 12885.

32 CFR Ch. XX (7-1-11 Edition)

menting regulations, internal rules, or guidelines, as necessary, to ensure consistency with NISP policies and procedures. Such reviews should normally occur during routine oversight visits, when there is indication of a problem that comes to the attention of the Director, ISOO, or after a change in national policy that impacts such regulations, rules, or guidelines. The Director, ISOO, shall provide findings from such reviews to the responsible department or agency.

§ 2004.12 Reviews by ISOO [102(b)(4)].

The Director, ISOO, shall fulfill his monitoring role based, in part, on information received from NISP Policy Advisory Committee (NISPPAC) members, from on-site reviews that ISOO conducts under the authority of EO 12829, as amended, and from complaints and suggestions from persons within or outside the Government. Findings shall be reported to the responsible department or agency.

Subpart B—Operations

§ 2004.20 National Industrial Security Program Operating Manual (NISPOM) [201(a)].

(a) The NISPOM applies to release of classified information during all phases of the contracting process.

(b) As a general rule, procedures for safeguarding classified information by contractors and recommendations for changes shall be addressed through the NISPOM coordination process that shall be facilitated by the Executive Agent. The Executive Agent shall address NISPOM issues that surface from industry, Executive Branch departments and agencies, or the NISPPAC. When consensus cannot be achieved through the NISPOM coordination process, the issue shall be raised to the NSC for resolution.

§ 2004.21 Protection of Classified Information [201(e)].

Procedures for the safeguarding of classified information by contractors are promulgated in the NISPOM. DoD, as the Executive Agent, shall use standards applicable to agencies as the basis for the requirements, restrictions, and safeguards contained in the

NISPOM; however, the NISPOM requirements may be designed to accommodate as necessary the unique circumstances of industry. Any issue pertaining to deviation of industry requirements in the NISPOM from the standards applicable to agencies shall be addressed through the NISPOM coordination process.

§ 2004.22 Operational Responsibilities [202(a)].

(a) *Designation of Cognizant Security Authority (CSA)*. The CSA for a contractor shall be determined by the preponderance of classified contract activity per agreement by the CSAs. The responsible CSA shall conduct oversight inspections of contractor security programs and provide other support services to contractors as necessary to ensure compliance with the NISPOM and that contractors are protecting classified information as required. DoD, as Executive Agent, shall serve as the CSA for all Executive Branch departments and agencies that are not a designated CSA. As such, DoD shall:

(1) Provide training to industry to ensure that industry understands the responsibilities associated with protecting classified information.

(2) Validate the need for contractor access to classified information, shall establish a system to request personnel security investigations for contractor personnel, and shall ensure adequate funding for investigations of those contractors under Department of Defense cognizance.

(3) Maintain a system of eligibility and access determinations of contractor personnel.

(b) *General Responsibilities*. Executive Branch departments and agencies that issue contracts requiring industry to have access to classified information and are not a designated CSA shall:

(1) Include the Security Requirements clause, 52.204-2, from the FAR in such contracts;

(2) Incorporate a Contract Security Classification Specification (DD 254) into the contracts in accordance with the FAR subpart 4.4;

(3) Sign agreements with the Department of Defense as the Executive Agent for industrial security services; and,

(4) Ensure applicable department and agency personnel having NISP implementation responsibilities are provided appropriate education and training.

(c) *National Interest Determinations (NIDs)*. Executive branch departments and agencies shall make a National Interest Determination (NID) before authorizing contractors, cleared or in process for clearance under a Special Security Agreement (SSA), to have access to proscribed information. To make a NID, the agency shall assess whether release of the proscribed information is consistent with the national security interests of the United States.

(1) The requirement for a NID applies to new contracts, including pre-contract activities in which access to proscribed information is required, and to existing contracts when contractors are acquired by foreign interests and an SSA is the proposed foreign ownership, control, or influence mitigation method.

(i) If access to proscribed information is required to complete pre-contract award actions or to perform on a new contract, the Government Contracting Activity (GCA) shall determine if release of the information is consistent with national security interests.

(ii) For contractors that have existing contracts that require access to proscribed information, have been or are in the process of being acquired by foreign interests, and have proposed an SSA to mitigate foreign ownership, the Cognizant Security Agency (CSA), or when delegated, the Cognizant Security Office (CSO) shall notify the GCA of the need for a NID.

(iii) The GCA(s) shall determine, within 30 days, per §2004.22(c)(4)(i), or 60 days, per §2004.22(c)(4)(ii), whether release of the proscribed information is consistent with national security interests unless the GCA requires additional time for the NID process due to special circumstances. The GCA shall formally advise the CSA, if special circumstances apply.

(2) In accordance with 10 U.S.C. 2536, DoD and the Department of Energy (DOE) cannot award a contract involving access to proscribed information to a contractor effectively owned or controlled by a foreign government unless