Information Security Oversight Office, NARA

§ 2004.11

Subpart A—Implementation and Oversight

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

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 implementing regulations, internal rules, or

---

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

§ 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.

§ 2004.23 Cost Reports [203(d)].

(a) The Executive Branch departments and agencies shall provide information each year to the Director, ISOO, on the costs within the agency associated with implementation of the NISP for the previous year.

(b) The DoD as the Executive Agent shall develop a cost methodology in coordination with industry to collect the costs incurred by contractors of all Executive Branch departments and agencies to implement the NISP, and shall report those costs to the Director, ISOO, on an annual basis.


(a) “Cognizant Security Agencies (CSAs)” means the Executive Branch departments and agencies authorized in EO 12829, as amended, to establish industrial security programs: The Department of Defense, designated as the Executive Agent; the Department of Energy; the Nuclear Regulatory Commission; and the Central Intelligence Agency.

(b) “Contractor” means any industrial, education, commercial, or other entity, to include licensees or grantees that has been granted access to classified information. Contractor does not include individuals engaged under personal services contracts.
# CHAPTER XXI—NATIONAL SECURITY COUNCIL

<table>
<thead>
<tr>
<th>Part</th>
<th>Rule Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2102</td>
<td>Rules and regulations to implement the Privacy Act of 1974</td>
<td>543</td>
</tr>
<tr>
<td>2103</td>
<td>Regulations to implement E.O. 12065—including procedures for public access to documents that may be declassified</td>
<td>546</td>
</tr>
</tbody>
</table>