CFR part or section where identified and described	Current OMB control No.
* * * * *	
1.338(i)–1	1545–1990
* * * * *	
1.381(c)(22)–1	1545–1990
* * * * *	
1.1060–1	1545–1658 1545–1990
* * * * *	

Mark E. Matthews,

Deputy Commissioner for Services and Enforcement.

Approved: March 7, 2006.

Eric Solomon,

Acting Deputy Assistant Secretary of the Treasury (Tax Policy).

[FR Doc. 06–3320 Filed 4–7–06; 8:45 am]

BILLING CODE 4830–01–P

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Information Security Oversight Office

32 CFR Part 2004

RIN 3095–AB34

National Industrial Security Program Directive No. 1

AGENCY: Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA).

ACTION: Final rule.

SUMMARY: The Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA), is publishing this Directive pursuant to section 102(b)(1) of Executive Order 12829, as amended, relating to the National Industrial Security Program. This order establishes a National Industrial Security Program (NISP) to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Redundant, overlapping, or unnecessary requirements impede those interests. Therefore, the NISP serves as the single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests. This Directive sets forth guidance to agencies to set uniform standards throughout the NISP that promote these objectives.

DATED: *Effective Date:* May 10, 2006.

FOR FURTHER INFORMATION CONTACT: J. William Leonard, Director, ISOO, at 202–357–5250.

SUPPLEMENTARY INFORMATION: The proposed rule was published in the January 27, 2006, **Federal Register** (71 FR 4541) for a 45-day public comment period. NARA received no comments on the proposed rule. The final rule is published without change.

This final rule is being issued pursuant to the provisions of section 102(b)(1) of Executive Order 12829, January 6, 2003 (58 FR 3479), as amended by Executive Order 12885, December 14, 1993, (58 FR 65863). The purpose of this Directive is to assist in implementing the Order; users of the Directive shall refer concurrently to that Order for guidance. As of November 17, 1995, ISOO became a part of NARA. The drafting, coordination, and issuance of this Directive fulfills one of the responsibilities of the implementation delegated to the ISOO Director. ISOO maintains oversight over Executive Order 12958, as amended, and policy oversight over Executive Order 12829, as amended. Nothing in this directive shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.), or the authority of the Director of Central Intelligence under the National Security Act of 1947, as amended, or Executive Order No. 12333 of December 8, 1981, or the authority of the Director of National Intelligence under the Intelligence Reform and Terrorism Prevention Act of 2004. Requirements of the latter Act will necessitate additional future changes to Executive Order 12829 and this implementing Directive. The interpretive guidance contained in this rule will assist agencies in implementing Executive Order 12829, as amended.

This rule is not a significant regulatory action for the purposes of Executive Order 12866. The rule is not a major rule as defined in 5 U.S.C. Chapter 8, Congressional Review of Agency Rulemaking. As required by the Regulatory Flexibility Act, we certify that this rule will not have a significant impact on a substantial number of small entities because it applies only to Federal agencies.

List of Subjects in 32 CFR Part 2004

Classified information.

■ 1. For the reasons set forth in the preamble, NARA amends Title 32 of the Code of Federal Regulations to add part 2004 as follows:

PART 2004—NATIONAL INDUSTRIAL SECURITY PROGRAM DIRECTIVE NO. 1

Subpart A—Implementation and Oversight

Subpart B—Operations

Authority: Section 102(b)(1) of Executive Order 12829, January 6, 2003, 58 FR 3479, as amended by Executive Order 12885, December 14, 1993, 58 FR 65863.

Subpart A—Implementation and Oversight

§ 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

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

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 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.

§ 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.

§ 2004.24 Definitions.

(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.

Dated: March 31, 2006.

J. William Leonard,

Director, Information Security Oversight Office.

Approved: March 31, 2006.

Allen Weinstein,

Archivist of the United States.

[FR Doc. 06–3383 Filed 4–7–06; 8:45 am]

BILLING CODE 7515–01–P

DEPARTMENT OF VETERANS AFFAIRS

38 CFR Part 20

RIN 2900–AM31

Board of Veterans' Appeals: Rules of Practice: Public Availability of Board Decisions

AGENCY: Department of Veterans Affairs.

ACTION: Final rule.

SUMMARY: The Department of Veterans Affairs (VA) is amending the Board of Veterans' Appeals (Board) Rules of Practice as relates to public availability of Board decisions, to set forth the current methods for archiving and retrieving Board decisions for public use. Due to advances in technology, Board decisions issued on or after January 1, 1992, are currently available in redacted form for public inspection and copying on Web sites that are accessible through the Internet. This is an improvement from the past practice