being. NIST will follow guidance issued by the National Institutes of Health at *http://ohrp.osophs.dhhs.gov/humansubjects/guidance/stemcell.pdf* for funding such research.

Research Projects Involving Vertebrate Animals: Any proposal that includes research involving vertebrate animals must be in compliance with the National Research Council's ''Guide for the Care and Use of Laboratory Animals'' which can be obtained from National Academy Press, 2101 Constitution Avenue, NW., Washington, DC 20055. In addition, such proposals must meet the requirements of the Animal Welfare Act (7 U.S.C. 2131 *et seq.*), 9 CFR parts 1, 2, and 3, and if appropriate, 21 CFR part 58. These regulations do not apply to proposed research using pre-existing images of animals or to research plans that do not include live animals that are being cared for, euthanized, or used by the project participants to accomplish research goals, teaching, or testing. These regulations also do not apply to obtaining animal materials from commercial processors of animal products or to animal cell lines or tissues from tissue banks.

Limitation of Liability: In no event will the Department of Commerce be responsible for proposal preparation costs if these programs fail to receive funding or are cancelled because of other agency priorities. Publication of this announcement does not oblige the agency to award any specific project or to obligate any available funds.

Executive Order 12866: This funding notice was determined to be not significant for purposes of Executive Order 12866.

Executive Order 13132 (Federalism): It has been determined that this notice does not contain policies with federalism implications as that term is defined in Executive Order 13132.

Executive Order 12372: Applications under this program are not subject to Executive Order 12372, ''Intergovernmental Review of Federal Programs.''

Administrative Procedure Act/ Regulatory Flexibility Act: Notice and comment are not required under the Administrative Procedure Act (5 U.S.C. 553) or any other law, for rules relating to public property, loans, grants, benefits or contracts (5 U.S.C. 553 (a)). Because notice and comment are not required under 5 U.S.C. 553, or any other law, for rules relating to public property, loans, grants, benefits or contracts (5 U.S.C. 553(a)), a Regulatory Flexibility Analysis is not required and has not been prepared for this notice, 5 U.S.C. 601 et seq.

Dated: March 23, 2006.

Hratch G. Semerjian,

Deputy Director.

[FR Doc. E6–4723 Filed 3–30–06; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 050601149–5323–02]

Announcing Approval of Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's approval of Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems. The use of FIPS 200 is compulsory and binding on federal agencies for: (i) All information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). FIPS 200 was developed to complement similar standards for national security systems.

DATES: This standard is effective March 31, 2006.

FOR FURTHER INFORMATION CONTACT: Dr. Ron Ross, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930, telephone (301) 975–5390, e-mail: *ron.ross@nist.gov.*

A copy of FIPS 200 is available electronically from the NIST Web site at: *http://csrc.nist.gov/publications/.*

SUPPLEMENTARY INFORMATION: The Federal Information Security Management Act (FISMA) requires all federal agencies to develop, document and implement agency-wide information security programs and to provide information security for the information and information systems that support the operations and assets of the agency, including those systems provided or managed by another agency, contractor, or other source.

To support agencies conducting their information security program, the FISMA called for NIST to develop federal standards for the security categorization of federal information and information systems according to risk levels, and four minimum security requirements for information and information systems in each security category. FIPS 199, Standards for the Security Categorization of Federal Information and Information Systems, issued in February 2004, was the first standard that was specified by the FISMA. FIPS 199 requires agencies to categorize their information and information systems as low-impact, moderate-impact, or high impact for the security objectives of confidentiality, integrity, and availability.

FIPS 200, which is the second standard that was specified by the FISMA, is an integral part of the risk management framework that NIST has developed to assist federal agencies in providing appropriate levels of information security based on levels of risk. In applying the provisions of FIPS 200, agencies will categorize their systems as required by FIPS 199, and then select an appropriate set of security controls from NIST Special Publication 800–53, Recommended Security Controls for Federal Information Systems, to satisfy their minimum security requirements.

On July 15, 2005, a notice was published in the **Federal Register** (Volume 70, Number 135, 40983–40984) announcing proposed FIPS 200 and soliciting comments on the proposed standard from the public, research communities, manufacturers, voluntary standards organizations, and federal, state, and local government organizations. In addition to being published in the **Federal Register**, the notice was posted on the NIST web pages. Information was provided about the submission of electronic comments.

Comments, responses, and questions were received from 13 private sector organizations, groups, or individuals and from 14 federal government organizations.

Most of the comments that were received recommended editorial changes; suggested the addition of references; provided general comments concerning the standard and its implementation; and asked questions concerning the implementation of the standard and the use of waivers. Some of the comments expressed concurrence with the standard as proposed, supported the intent, goals, and

presentation of the standard, and complimented NIST on the document. No comments opposed the adoption of the standard.

The primary interests and issues that were raised in the comments included: Time needed for implementation; inclusion of waiver provisions; inclusion of additional references; rearrangement and indexing of the text; addition of text and implementation details already available in other NIST publications; and expansion of definitions.

All of the editorial suggestions and recommendations were carefully reviewed, and changes were made to the standard where appropriate. The text of the standard, the terms and definitions listed in the standard, the references and the footnotes were modified as needed.

Following is an analysis of the major editorial, implementation and related comments that were received.

Comment: Some comments recommended changing the requirement that federal agencies must be in compliance with the standard not later than one year from its effective date. The recommendations received suggested both lengthening the time for compliance because of concerns about the cost of implementing the standard within budget constraints, and shortening the time for compliance to achieve improved security.

Response: NIST believes that the requirement for compliance not later than one year from effective date of the standard is reasonable, and that no changes are needed to either prolong or shorten the time for compliance with the standard.

Comment: A federal agency recommended that a provision be added to the standard to enable federal agencies to waive the standard when they lack sufficient resources to comply by the deadline.

Response: The Federal Information Security Management Act contains no provisions for agency waivers to standards. The FISMA states that information security standards, which provide minimum information security requirements and which are needed to improve the security of federal information and information systems, are required mandatory standards. The Secretary of Commerce is authorized to make information security standards compulsory and binding, and these standards may not be waived.

Comment: Comments were received about regrouping or indexing the seventeen security areas covered by the standard. FIPS 200 specifies minimum security requirements for federal information and information systems in seventeen security-related areas.

Response: NIST believes that indexing would be confusing and would add unnecessary complexity to the standard. The seventeen areas that are defined in the standard represent a broad-based, balanced information security program. The areas, which address the management, operational, and technical aspects of protecting federal information and information systems, are concise and do not require indexing.

Comment: One federal agency recommended that the standard specify a time period for retaining audit records.

Response: NIST believes that requirements about retention of audit records should be defined by agencies, and should not be specified in the standard.

Comment: Several comments suggested additions and changes to the standard concerning risk management procedures, audit controls, baseline security controls, and risks introduced by new technologies.

Response: A section of the proposed FIPS 200 covering these topics has been removed from the final version of the standard, and these comments will be considered when NIST Special Publication (SP) 800–53, Recommended Security Controls for Federal Information Systems, is updated. FIPS 200 specifies that federal agencies use SP 800–53 to select security controls that meet the minimum security requirements in the seventeen security-related areas. The security controls in SP 800–53 represent the current state-of-the-practice safeguards and countermeasures for information systems. NIST plans to review these security controls at least annually and to propose any changes needed to respond to experience gained from using the controls, changing security requirements within federal agencies, and new security technologies. Any changes or additions to the minimum security controls and the security control baselines described in SP 800–53 will be made available for public review before any modifications are made. Federal agencies will have up to one year from the date of the final publication to comply with the changes.

Comment: Some comments suggested the inclusion of expanded definitions for terms such as systems, major applications, and general support systems.

Response: NIST is adhering to the definition of system used in the Federal Information Security Management Act, and believes that attempts to further define these terms and to make distinctions between systems and applications may be confusing.

Comment: One federal agency asked about the security issues related to the use of computerized medical devices. Another commenter asked about inclusion of information on training and certification of information technology professionals.

Response: The issue of computerized medical devices may need to be addressed, but FIPS 200 is not the appropriate document. The issues of training information and the certification of information technology professionals are also outside the scope of FIPS 200.

Authority: Federal Information Processing Standards (FIPS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Pub. L. 104–106) and the Federal Information Security Management Act (FISMA) of 2002 (Pub. L. 107–347).

E.O. 12866: This notice has been determined to be not significant for the purposes of E.O. 12866.

Dated: March 23, 2006.

William Jeffrey,

Director.

[FR Doc. E6–4720 Filed 3–30–06; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

RIN 0693–AB56

[Docket No. 050825229–5308–02]

Announcing Approval of Federal Information Processing Standard (FIPS) Publication 201–1, Standard for Personal Identity Verification of Federal Employees and Contractors

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's approval of Federal Information Processing Standard (FIPS) Publication 201–1, Standard for Personal Identity Verification of Federal Employees and Contractors. The changes to Section 2.2, PIV Identify Proofing and Registration Requirements, Section 4.3, Cryptographic Specifications, Section 5.2, PIV Identity Proofing and Registration Requirements, and to Section 5.3.1, PIV Card Issuance, clarify the identity proofing and registration process that departments and agencies