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

should follow when issuing identity credentials. These changes are needed to make FIPS 201–1 consistent with the Memorandum for All Departments and Agencies (M–05–24), issued by the Office of Management and Budget on August 5, 2005, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors.

DATES: The approved changes are effective as of March 31, 2006.

ADDRESSES: The approved changes to FIPS Publication 201–1 are available electronically from the NIST Web site at: *http://csrc.nist.gov/piv-program/*. Comments that were received on the proposed changes will also be published electronically at *http://csrc.nist.gov/piv-program/*.

FOR FURTHER INFORMATION CONTACT: W. Curtis Barker, (301) 975–8443, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930, e-mail: *wbarker@nist.gov.*

Information about FIPS 201–1 and the PIV program is available on the NIST Web pages: *http://csrc.nist.gov/piv-program/.*

SUPPLEMENTARY INFORMATION: A **Federal Register** notice (70 FR 17975–78) on April 8, 2005, announced that the Secretary of Commerce had approved FIPS Publication 201, Standard for Personal Identity Verification of Federal Employees and Contractors. HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 27, 2004, directed the Secretary of Commerce to promulgate, by February 27, 2005, a Government-wide standard for secure and reliable forms of identification to be issued to Federal government employees and contractors (including contractor employees).

FIPS 201 was effective on February 25, 2005, and was made compulsory and binding on Federal agencies for use in issuing a secure and reliable form of personal identification to employees and contractors. The standard does not apply to personal identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

A notice was published in the **Federal Register** (70 FR 53346–47) on September 8, 2005, announcing the proposed changes to FIPS 201. The primary goal for the changes are to make FIPS 201–1 consistent with the Memorandum for All Departments and Agencies (M–05–24), issued by the Office of Management and Budget on August 5, 2005, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors.

The **Federal Register** notice solicited comments on the draft 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 and an electronic template for the submission of comments was made available.

Comments, responses, and questions were received from private sector organizations, groups, or individuals, and Federal government organizations. These comments have all been made available by NIST at *http://csrc.nist.gov/piv-program/*. Following is an analysis of the comments received, including the interests, concerns, recommendations, and issues considered in the development of FIPS 201–1.

Comment: The requirement to include electronically distinguishable NACI indicator in the identity credential should apply to PIV–II only.

Response: NIST agrees that the NACI indicator does not apply to PIV–1. Moved this requirement to Section 5.2 of FIPS 201–1.

Comment: The exact nature of the electronically distinguishable feature must be defined to ensure adequate interoperability.

Response: NIST specified implementation of the NACI Interim Indicator in the PIV Authentication certificate and updated Section 4.3, Section 5.4.2.1, and the PIV Certificate definition Appendix. Specifically, the Interim Indicator shall be implemented as a non-critical private extension in the PIV Authentication certificate.

Comment: Agencies do not support 5-day waiting period for the completion of the NAC. Agencies strongly disagree with the requirement for the NAC completion prior to an employee or contractor receiving a credential or access to federally controlled facilities or logical access to federally controlled information system. Moreover, agencies believed that the NAC results will not be received within five days in a majority of the cases. In that regard, the agency leadership must delay the hiring process for five additional days with no concomitant security benefit.

Response: NIST removed specific waiting period and NAC without written inquiries as a qualifier in Section 2.2 of FIPS 201–1. The five-day waiting period did introduce artificial delay in the routine card issuance. As a result, pending receipt of the results of the NACI, an agency may issue an identity credential based on the FBI National Criminal History Check (fingerprint check).

Comment: Agencies do not support the inclusion of a NACI indicator within the identity credential. Agencies believe this requirement will be costly to implement because the requirement would require facilities to alter or replace the identity credential when the NAC is complete. They recommend further analysis regarding the intended use, CONOPS, and benefits for this distinguishable element within the identity credential is required before their acceptance.

Response: This requirement is imposed to be consistent with the OMB memorandum M–05–24. The NACI indicator relays the rigor of identity proofing completed on the PIV cardholder when the card was issued. The relying parties, such as federal agencies, may require NACI completion to allow access to their resources. The NACI indicator will enable agencies to make an informed decision about the cardholders binding to the identity credentials.

Authority: In accordance with 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), the Secretary of Commerce is authorized to approve Federal Information Processing Standards (FIPS). Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 27, 2004, directed the Secretary of Commerce to promulgate, by February 27, 2005, a Government-wide standard for secure and reliable forms of identification to be issued to Federal government employees and contractors.

E.O. 12866: This notice has been determined to be significant for the purposes of E.O. 12866.

Dated: March 23, 2006.

William Jeffrey,

Director.

[FR Doc. E6–4722 Filed 3–30–06; 8:45 am]

BILLING CODE 3510–CN–P