the security controls necessary to satisfy the minimum requirements.

Prior to the submission of this proposed standard to the Secretary of Commerce for review and approval, it is essential that consideration be given to the needs and views of the general public, the information technology industry, and federal, state, and local government organizations. The purpose of this notice is to solicit such views.

DATES: Comments must be received on or before 5 p.m., September 13, 2005.

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Comments on Draft FIPS Publication 200, 100 Bureau Drive (Stop 8930), National Institute of Standards and Technology, Gaithersburg, MD 20899–8930. Comments may also be sent via electronic mail to: *draftfips200@nist.gov*.

A copy of draft FIPS Publication 200 is available from the NIST Web site at: *http://csrc.nist.gov/publications/fips/index.html*.

Comments received in response to this notice will be published at *http://csrc.nist.gov*.

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

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 in conducting their information security programs, the FISMA called for NIST to develop federal standards for the security categorization of federal information and information systems according to risk levels, and for minimum security requirements for information and information systems in each security category. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, issued in February 2004, is the first standard that was specified by the FISMA. FIPS Publication 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.

Draft FIPS Publication 200, 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. FIPS Publication 200 specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements. In applying the provisions of FIPS Publication 200, agencies will categorize their information systems as required by FIPS Publication 199, and subsequently select an appropriate set of security controls from NIST Special Publication 800–53, Recommended Security Controls for Federal Information Systems, to satisfy the minimum security requirements. Issued in February 2005, NIST Special Publication 800–53 defines minimum security controls needed to provide cost-effective protection for low-impact, moderate-impact, and high-impact information systems and the information processed, stored, and transmitted by those systems.

The proposed standard will be applicable to: (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). The standard has been broadly developed from a technical perspective to complement similar standards for national security systems. In addition to the agencies of the federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States are encouraged to consider the use of this standard, as appropriate.

Proposed FIPS Publication 200 specifies minimum security requirements for federal information and information systems in seventeen security-related areas that represent a broad-based, balanced information security program. The seventeen security-related areas encompass the management, operational, and technical aspects of protecting federal information and information systems, and include: access control; audit and accountability; awareness and training; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; personnel security; physical and environmental protection; planning; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

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 and the Federal Information Security Management Act of 2002 (Public Law 107–347).

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

Dated: July 7, 2005.

Hratch G. Semerjian,

Acting Director, NIST.

[FR Doc. 05–13994 Filed 7–14–05; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 050329087–5087–01]

Proposed Withdrawal of Ten (10) Federal Information Processing Standards (FIPS)

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

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) proposes to withdraw ten (10) Federal Information Processing Standards (FIPS) from the FIPS series. The standards proposed for withdrawal include FIPS 161–2, FIPS 183, FIPS 184, FIPS 192 and 192–1, which adopt voluntary industry standards for Federal government use. These FIPS are obsolete because they have not been updated to reference current or revised voluntary industry standards. In addition, FIPS 4–2, FIPS 5–2, FIPS 6–4, and FIPS 10–4, adopt specifications or data standards that are developed and maintained by other Federal government agencies or by voluntary industry standards organizations. These FIPS have not been updated to reflect

the changes and modifications that have been made by the organizations that develop and maintain the specifications and data representations. FIPS 113, Computer Data Authentication, specifies an algorithm for generating and verifying a Message Authentication Code (MAC). Since the algorithm is based on the Data Encryption Standard, which has been recommended for withdrawal, NIST plans to recommend the use of newer techniques for data authentication based on more secure algorithms.

Prior to the submission of this proposed withdrawal of FIPS to the Secretary of Commerce for review and approval, NIST invites comments from the public, users, the information technology industry, and Federal, State and local governments government organizations concerning the withdrawal of the FIPS.

DATES: Comments on the proposed withdrawal of the FIPS must be received no later than 5 p.m. on October 13, 2005.

ADDRESSES: Written comments concerning the withdrawal of the FIPS should be sent to: Information Technology Laboratory, ATTN: Proposed Withdrawal of 10 FIPS, Mail Stop 8930, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899. Electronic comments should be sent to: *fips.comments@nist.gov*.

Information about the FIPS is available on the NIST Web pages: *http://www.itl.nist.gov/fipspubs/index.htm*.

Comments received in response to this notice will be published electronically at *http://csrc.nist.gov/publications/fips/index.html*.

FOR FURTHER INFORMATION CONTACT: Ms. Shirley M. Radack, telephone (301) 975–2833, MS 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899 or via e-mail at *shirley.radack@nist.gov*.

SUPPLEMENTARY INFORMATION: The following Federal Information Processing Standards (FIPS) Publications are proposed for withdrawal from the FIPS series:

FIPS 4–2, Representation of Calendar Date to Facilitate Interchange of Data Among Information Systems.

FIPS 5–2, Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas.

FIPS 6–4, Counties and Equivalent Entities of the U.S., Its Possessions, and Associated Areas.

FIPS 10–4, Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions.

FIPS 113, Computer Data Authentication.

FIPS 161–2, Electronic Data Interchange (EDI).

FIPS 183, Integration Definition for Function Modeling (IDEF0).

FIPS 184, Integration Definition for Information Modeling (IDEFIX).

FIPS 192, Application Profile for the Government Information Locator Service (GILS).

FIPS 192–1 (a)&(b), Application Profile for the Government Information Locator Service (GILS).

These FIPS are being proposed for withdrawal because they are obsolete, or have not been updated to adopt current voluntary industry standards, federal specifications, or federal data standards. Federal agencies are responsible for using current voluntary industry standards and current federal specifications and data standards in their acquisition and management activities.

The Information Technology Management Reform Act of 1996 (Division E of Pub. L. 104–106) and Executive Order 13011 emphasize agency management of information technology and Government-wide interagency support activities to improve productivity, security, interoperability, and coordination of Government resources. Under the National Technology Transfer and Advancement Act of 1995 (Pub. L. 104–113) Federal agencies and departments are directed to use technical standards that are developed in voluntary consensus standards bodies. Voluntary industry standards are the preferred source of standards to be used by the Federal government. The use of voluntary industry standards eliminates the cost to the government of developing its own standards, and furthers the policy of reliance upon the private sector to supply goods and services to the government. Federal Information Processing Standards (FIPS) are developed only when interoperability of different systems, for the portability of data and software, and for computer security.

FIPS 161–2, FIPS 183, and FIPS 184 are voluntary consensus standards, and current versions of these specifications are available from voluntary standards organizations.

FIPS 192 and 192–1 are being withdrawn because agencies use commercial sources to aid citizens in locating government information.

Per Section 207(d) of the E-Government Act of 2002, OMB will issue policies requiring agencies use standards, which are open to the maximum extent feasible and interoperable across agencies, to enable effective categorization and organization of Government information in a way that is searchable electronically, including by searchable identifiers.

The policy will define categories of Government information which shall be required under the standards so agencies can continue to use aids, including Federal or nonfederal sources, for locating agency information dissemination products to reasonably achieve agency information dissemination objectives.

FIPS 4–2, FIPS 5–2, FIPS 6–4, and FIPS 10–4 are Federal data standards and specifications that have been and will continue to be developed and maintained by Federal government agencies other than NIST. Current versions of these data standards and specifications are available through the developing Federal agencies' web pages. NIST will keep references to these withdrawn FIPS on its FIPS web pages, and will link to current versions of these standards and specifications where appropriate.

Withdrawal means that these FIPS would no longer be part of a subscription service that is provided by the National Technical Information Service. NIST will continue to provide relevant information on standards and guidelines by means of electronic dissemination methods.

Authority: Federal Information Processing Standards Publications (FIPS PUBS) 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 of 2002 (Pub. L. 107–347).

Classification: Executive Order 12866: This notice has been determined not to be significant for the purposes of Executive Order 12866.

Dated: July 11, 2005.

Hratch G. Semerjian,

Acting Director, NIST.

[FR Doc. 05–13992 Filed 7–14–05; 8:45 am]

BILLING CODE 3510–CN–P