

themes. There will also be breakouts for each subcommittee to meet individually. The agenda may change to accommodate Committee business. The final agenda will be posted on the Smart Grid Web site at <http://www.nist.gov/smartgrid>.

**DATES:** The SGAC will hold a meeting on Thursday, March 24, 2011, from 8:30 a.m. until 5 p.m. The meeting will be open to the public.

**ADDRESSES:** The meeting will be held in the Lecture Room C, in the Administration Building at NIST in Gaithersburg, Maryland. Please note admittance instructions under the **SUPPLEMENTARY INFORMATION** section of this notice.

**FOR FURTHER INFORMATION CONTACT:** Dr. George W. Arnold, National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8100, Gaithersburg, MD 20899-8100; telephone 301-975-2232, fax 301-975-4091; or via e-mail at [nistsgfac@nist.gov](mailto:nistsgfac@nist.gov).

**SUPPLEMENTARY INFORMATION:** The Committee was established in accordance with the Federal Advisory Committee Act (5 U.S.C. App.).

Background information on the Committee is available at <http://www.nist.gov/smartgrid/committee.cfm>.

Pursuant to the Federal Advisory Committee Act, 5 U.S.C. App., notice is hereby given that the Smart Grid Advisory Committee (SGAC) will hold a meeting on Thursday, March 24, 2011, from 8:30 a.m. until 5 p.m. The meeting will be held in the Lecture Room C, in the Administration Building at NIST in Gaithersburg, Maryland. The primary purpose of this meeting is to review the early findings and observations of each Subcommittee, strategize the Table of Contents for the Committee report to NIST, agree on the page limit for each subcommittee, and look for any common overarching themes. There will also be breakouts for each subcommittee to meet individually. The agenda may change to accommodate Committee business. The final agenda will be posted on the Smart Grid Web site at <http://www.nist.gov/smartgrid>.

Individuals and representatives of organizations who would like to offer comments and suggestions related to the Committee's affairs are invited to request a place on the agenda by contacting Cuong Nguyen at [cuong.nguyen@nist.gov](mailto:cuong.nguyen@nist.gov) or (301) 975-2254 no later than March 17, 2011. On March 24, 2011, approximately one-half hour will be reserved at the end of the meeting for public comments, and speaking times will be assigned on a first-come, first-serve basis. The amount

of time per speaker will be determined by the number of requests received, but is likely to be about 3 minutes each. Questions from the public will not be considered during this period. Speakers who wish to expand upon their oral statements, those who had wished to speak but could not be accommodated on the agenda, and those who were unable to attend in person are invited to submit written statements to the Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8100, Gaithersburg, MD 20899-8100; fax 301-975-4091; or via e-mail at [nistsgfac@nist.gov](mailto:nistsgfac@nist.gov).

All visitors to the NIST site are required to pre-register to be admitted. Anyone wishing to attend this meeting must register by close of business Thursday, March 17, 2011, in order to attend. Please submit your name, time of arrival, e-mail address, and phone number to Cuong Nguyen. Non-U.S. citizens must also submit their country of citizenship, title, employer/sponsor, and address. Mr. Nguyen's e-mail address is [cuong.nguyen@nist.gov](mailto:cuong.nguyen@nist.gov) and his phone number is (301) 975-2254.

Dated: March 2, 2011.

**Charles H. Romine,**  
*Acting Associate Director for Laboratory Programs.*

[FR Doc. 2011-5250 Filed 3-7-11; 8:45 am]

**BILLING CODE 3510-13-P**

## DEPARTMENT OF COMMERCE

### National Institute of Standards and Technology

[Docket No. 110124059-1058-02]

#### Announcing Draft Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification of Federal Employees and Contractors Standard, Request for Comments, and Public Workshop on Draft FIPS 201-2

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

**ACTION:** Notice and request for comments.

**SUMMARY:** The National Institute of Standards and Technology (NIST) publishes this notice to request comments on Draft Federal Information Processing Standard (FIPS) Publication 201-2, "Personal Identity Verification of Federal Employees and Contractors Standard." Draft FIPS 201-2 amends FIPS 201-1 and includes clarifications of existing text, removal of conflicting requirements, additional text to improve clarity, adaptation to changes in the

environment since the publication of FIPS 201-1, and specific changes requested by Federal agencies and implementers. NIST has received numerous change requests, some of which, after analysis and coordination with the Office of Management and Budget (OMB) and United States Government (USG) stakeholders, are incorporated in the Draft FIPS 201-2. Before recommending FIPS 201-2 to the Secretary of Commerce for review and approval, NIST invites comments from the public concerning the proposed changes. NIST will hold a public workshop at NIST in Gaithersburg, MD to present the Draft FIPS 201-2. Please see admittance instructions in the **SUPPLEMENTARY INFORMATION** section below.

**DATES:** Comments must be received by June 6, 2011. The public workshop will be held on April 18-19, 2011. Pre-registration must be completed by close of business on April 11, 2011.

**ADDRESSES:** Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, ATTN: Comments on Revision Draft FIPS 201-1, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899. Electronic comments may be sent to: [piv\\_comments@nist.gov](mailto:piv_comments@nist.gov). Anyone wishing to attend the workshop in person, must pre-register at <http://www.nist.gov/allevvents.cfm>. Additional workshop details and webcast will be available on the NIST Computer Security Resource Center Web site at <http://csrc.nist.gov>.

**FOR FURTHER INFORMATION CONTACT:** William MacGregor, (301) 975-8721, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930, e-mail: [william.macgregor@nist.gov](mailto:william.macgregor@nist.gov), or Hildegard Ferraiolo, (301) 975-6972, e-mail: [hildegard.ferraiolo@nist.gov](mailto:hildegard.ferraiolo@nist.gov), or Ketan Mehta, (301) 975-8405, e-mail: [ketan.mehta@nist.gov](mailto:ketan.mehta@nist.gov).

**SUPPLEMENTARY INFORMATION:** FIPS 201 was issued in February 2005, and in accordance with NIST policy was due for review in 2010. In consideration of changes in the environment over the last five years and specific requests for changes from USG stakeholders, NIST determined that a revision of FIPS 201-1 (version in effect) is warranted. NIST has received numerous change requests, some of which, after analysis and coordination with OMB and USG stakeholders, are incorporated in the Draft FIPS 201-2. Other change requests

incorporated in the Draft FIPS 201–2 result from the 2010 Business Requirements Meeting held at NIST. The meeting focused on business requirements of Federal departments and agencies. The following is a summary of changes reflected in the Draft FIPS 201–2. Please note that the proposed revision of the document has caused a renumbering of several sections of FIPS 201–1 (version in effect). The section references below are consistent with Draft FIPS 201–2. The changes in Draft FIPS 201–2 are:

- Changes to clarify requirements and editorial corrections are incorporated throughout the document. These changes are not intended to modify the substantive requirements in FIPS 201–1.

- Specific modifications that potentially change an existing requirement or add a new requirement are reflected in the following list.

—In Section 2.1, the second bullet is *replaced* with “A credential is issued only after the National Agency Check with Written Inquiries (NACI) or equivalent is initiated and the FBI National Criminal History Check (NCHC) is completed,” to eliminate an inconsistency that was inadvertently introduced by the FIPS 201–1 revision.

—In Section 2.2, the text is *replaced* with a reference to the memorandum from Linda Springer, Director Office of Personnel Management (OPM), dated 31 July 2008, “Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD–12.” The purpose of this change is to update the identity credentialing requirements in accordance with OPM guidance issued after the FIPS 201–1 was published.

—Section 2.3 is *modified* to directly incorporate the content from the I–9 form that is relevant to FIPS 201. This change is made to eliminate confusion that has resulted from I–9 content that is not used by FIPS 201–1 processes; it also provides a more precise requirement statement for the two forms of identity source documents.

—Section 2.3 is *modified* to introduce the concept of a “chain-of-trust,” maintained by a PIV Card Issuer, further described in Sections 2.4, 2.5 and 4.4.1. The “chain-of-trust” allows the holder of a PIV Card to obtain a replacement for a compromised, lost, stolen, or damaged PIV Card through biometric authentication. This capability is requested by Federal agencies because the alternative, complete re-enrollment, is time-consuming and expensive. The

“chain-of-trust” method can only be used if the PIV Card Issuer has retained biometric data through which an individual can be authenticated.

—Section 2.4 is *added* to define a 1-to-1 biometric match. A 1-to-1 biometric match is necessary to associate a presenting individual with their ‘chain-of-trust’ record. The objective is to reduce replacement cost to agencies for lost, stolen, or damaged PIV Cards, to reduce the amount of data gathering, and minimize in-person visits without compromising the security objectives of HSPD–12.

—Section 2.4 is *modified* to increase the maximum life of PIV Card from 5 years to 6 years. This revision is made in response to agency requests to synchronize lifecycles of card, certificates, and biometric data.

—Section 2.4.1 is *added* to introduce a special rule for pseudonyms, clarifying the conditions under which pseudonyms may be approved by the sponsoring agency (*i.e.*, for the protection of the cardholder). FIPS 201–1 does not specify requirements for issuing PIV credentials under pseudonyms. This use-case requires a normative list of minimum requirements within the standard.

—Section 2.4.2 is *added* to introduce a grace period for the period between termination of an employee or contractor and re-employment by the USG or a Federal contractor. If re-employment occurs within the grace period, to obtain a new PIV Card, an NCHC is required and a complete NACI is not required. For example, an employee may be detailed to a special assignment for a brief time period and, upon completion of the assignment, return to the original agency. In another case, the PIV Cardholder may move from one Federal agency to another within a short period of time. In each of these situations, repeating the entire identity proofing and identity vetting process when all the necessary information about the individual was previously collected in accordance with FIPS 201–1 is inefficient. The grace period to allow reuse of the existing records held by an agency addresses this inefficiency.

—Section 2.5 is *modified* to restructure the PIV Card maintenance procedures slightly. “Renewal” of a PIV Card to re-collect biometric data, currently a facial image and two fingerprint templates, is required once every twelve years, to update files to account for normal aging. Subsequent to the issuance of FIPS 201–1 and based on comments received by NIST,

it is apparent that terms such as “renewal”, “reissuance”, “replacement”, “registration”, etc., are used interchangeably and inaccurately and that FIPS 201–1 needs to clearly state the purpose and circumstances under which identity credential renewal is required. Draft FIPS 201–2 introduces normative text to address this ambiguity.

—Section 2.5.2.1 is *added* to recognize legal name changes. Name change is a very common occurrence, and it represents a major change in identity source documents. Specific requirements to manage and record legal name changes correctly and consistently across identity management systems were identified and are included.

—Sections 2.5.3 and 2.5.4 are *added* to provide requirements for post-issuance updates made to the PIV Card after it is issued to the cardholder. These requirements are added in response to agency requests.

—Section 2.5.5 is *added* to provide details on reset procedures for PIN, biometrics or other types of resettable data as per agency requests.

—Section 4.1.4 is *added* to provide visual card topography zones and color specifications from SP 800–104 “A Scheme for PIV Visual Card Topography.” SP 800–104 was developed after FIPS 201–1 was published to enhance the uniformity of colors and additional zones needed by agencies.

—Section 4.1.4.1 is *modified* to allow longer names (70 characters) to be printed on the card in the existing zone. This change is made to enable printing of complete names for required accuracy.

—Section 4.1.4.3 is *added* to provide requirements for compliance with Section 508 of the Americans with Disabilities Act. The U.S. Access Board, an independent Federal agency devoted to accessibility for people with disabilities, requested improvements in FIPS 201 to facilitate the use of the PIV Card by people with impaired vision or manual dexterity. For example, an improvement could allow an unsighted person to quickly and positively orient the card by touch when presenting the PIV Card to a card reader.

—Section 4.1.6.1 is *modified* to revise the list of mandatory and optional PIV logical credentials. This section is modified based on the inputs received during the 2010 Business Requirements Meeting described above. The section adds a requirement to collect alternate iris images when

an agency cannot capture reliable fingerprints. This section also specifies a mandatory asymmetric card authentication key as part of PIV logical credentials and adds an optional On-card biometric comparison as a means of performing card activation and PIV authentication mechanism. The section includes hooks for additional keys if they are needed for secure messaging. In addition, NIST proposes that specific key references and their use will be defined in a future special publication.

- Section 4.1.7.1 is *modified* to allow a PIN or equivalent verification data (e.g., biometric data) to activate a PIV Card to perform privileged operations. The requirement that all PIV System cryptographic modules be tested and validated to FIPS 140–2 Security Level 2 (logical) or Security Level 3 (physical) is not changed.
- Section 4.3 is *modified* to make the NACI Indicator optional and to deprecate its use. The NACI Indicator originally was included in the PIV Authentication Certificate to inform relying systems that the background investigation had not been completed before issuing the PIV Card. Since the issuance of FIPS 201–1, timely completion of background investigations has improved, online status checking services are now available, OPM requirements for background investigations have been revised, and OMB reporting requirements are in place. These improvements provide sufficient controls to make the need for storing NACI Indicator on the PIV Card optional and to deprecate its use.
- Section 4.3 is *modified* to add an option to include country(ies) of citizenship of Foreign Nationals in the PIV Authentication Certificate. This change reflects the desirability of electronically reading the affiliation of Foreign Nationals.
- Section 4.5.3 is *added* to allow a possible future inclusion of an optional ISO/IEC 24727 profile that enables middleware a degree of independence from credential interfaces and vice versa and thus provides adaptability and resilience to PIV card evolution.
- Sections 6.2.2, 6.2.3.1, and 6.2.3.2 are *modified* to remove the qualifier “(Optional)” from the requirement for signature verification and certificate path validation in the CHUID, BIO, and BIO–A authentication mechanisms. These signature verification and path validation functions would be mandatory under FIPS 201–2 to achieve the

authentication assurance confidence levels shown in Tables 6–2 and 6–3.

- Section 6.2.5 and 6.2.6 are *added* to provide authentication mechanisms based on optional PIV data elements. Specifically, an On-card biometric comparison authentication mechanism is added in Section 6.2.5 and a symmetric card authentication key authentication mechanism is added in Section 6.2.6.
- Appendix A is *removed*.

FIPS 201–1 and Draft FIPS 201–2 are available electronically from the NIST Web site at: <http://csrc.nist.gov/publications/fips/index/html>.

NIST will hold a public workshop on Draft FIPS 201–2 on Monday and Tuesday, April 18 and 19, 2011 at NIST in Gaithersburg, Maryland. The workshop may also be attended remotely via webcast. The agenda, webcast and related information for the public workshop will be available before the workshop on the NIST Computer Security Resource Center Web site at <http://csrc.nist.gov>. This workshop is not being held in anticipation of a procurement activity. Anyone wishing to attend the workshop in person, must pre-register at <http://www.nist.gov/allvents.cfm> by close of business Monday, April 11, 2011, in order to enter the NIST facility and attend the workshop. In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104–106) and the Federal Information Security Management Act of 2002 (FISMA) (Pub. L. 107–347), the Secretary of Commerce is authorized to approve Federal Information Processing Standards (FIPS). Homeland Security Presidential Directive (HSPD) 12, entitled “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 Federal standard for secure and reliable forms of identification (the ‘Standard’) \* \* \* ,” and further directed that the Secretary of Commerce “shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.”

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

Dated: February 17, 2011.

**Charles H. Romine,**  
*Acting Associate Director for Laboratory Programs.*

[FR Doc. 2011–5259 Filed 3–7–11; 8:45 am]

**BILLING CODE 3510–13–P**

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

#### Proposed Information Collection; Comment Request; Marianas Trench Marine National Monument Knowledge and Attitudes Survey

**AGENCY:** National Oceanic and Atmospheric Administration (NOAA), Commerce.

**ACTION:** Notice.

**SUMMARY:** The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

**DATES:** Written comments must be submitted on or before May 9, 2011.

**ADDRESSES:** Direct all written comments to Diana Hynek, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6616, 14th and Constitution Avenue, NW., Washington, DC 20230 (or via the Internet at [dHynek@doc.gov](mailto:dHynek@doc.gov)).

**FOR FURTHER INFORMATION CONTACT:** Requests for additional information or copies of the information collection instrument and instructions should be directed to Dr. Stewart Allen, (808) 944–2186 or [Stewart.Allen@noaa.gov](mailto:Stewart.Allen@noaa.gov).

#### SUPPLEMENTARY INFORMATION:

##### I. Abstract

President George W. Bush established the Marianas Trench Marine National Monument (Monument) on January 6, 2009, by Presidential Proclamation 8335. The monument includes approximately 95,216 square miles within three units in the Mariana Archipelago. The Mariana Trench Unit is almost 1,100 miles long and 44 miles wide and includes only the submerged lands. The Volcanic Unit consists of submerged lands around 21 undersea mud volcanoes and thermal vents along the Mariana Arc. The Islands Unit includes only the waters and submerged lands of the three northernmost Mariana Islands: Farallon de Pajaros or Uracas; Maug; and Asuncion, below the mean low water line. Within the Islands Unit of the monument, commercial fishing is prohibited but sustenance, recreational, and traditional indigenous fishing can be allowed on a sustainable basis.

The Secretary of the Interior has management responsibility for the monument, in consultation with the Secretary of Commerce who, through