Billing Code 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 130402311-3311-01]

Announcing Approval of Federal Information Processing Standard (FIPS) Publication 201-2, Personal Identity Verification (PIV) 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 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors. FIPS 201-2 includes clarifications to existing text, additional text in cases where there were ambiguities, adaptation to changes in the environment since the publication of FIPS 201-1, and specific changes requested by Federal agencies and implementers.

DATE: FIPS 201-2 is effective on [PLEASE INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: FIPS 201-2 is available electronically from the NIST web site at: *http://csrc.nist.gov/publications/PubsFIPS.html*. Comments that were received on the proposed changes will also be published electronically at *http://csrc.nist.gov/groups/SNS/piv/index.html*.

FOR FURTHER INFORMATION CONTACT: Hildegard Ferraiolo, (301) 975–6972, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: *hildegard.ferraiolo@nist.gov*, or David Cooper, (301) 975-3194, *david.cooper@nist.gov*.

SUPPLEMENTARY INFORMATION: FIPS 201 was issued on April 8, 2005 (70 FR 17975) in response to Homeland Security Presidential Directive 12 (HSPD-12), and in accordance with NIST policy was due for review in 2010. In consideration of technological advancements over the last five years and specific requests for changes from United States Government (USG) stakeholders, NIST determined that a revision of FIPS 201–1 (version in effect) was warranted. NIST received numerous change requests, some of which, after analysis and coordination with the Office of Management and Budget (OMB) and USG stakeholders, were incorporated in a proposed draft of FIPS 201–2 (‘‘2011 Draft’’). Other change requests incorporated in the 2011 Draft resulted from the 2010 Business Requirements Meeting held at NIST. The meeting focused on business requirements of federal departments and agencies. On March 8, 2011, a notice was published in the Federal Register (76 FR 12712), soliciting public comments on the 2011 Draft. During the

public comment period, a public workshop was held at NIST on April 18–19, 2011, in order to present the 2011 Draft. Comments and questions regarding the 2011 Draft were submitted by 46 entities, composed of 25 U.S. federal government organizations, two state government organizations, one foreign government organization, 16 private sector organizations, and two private individuals. NIST made significant changes to the 2011 Draft based on the public comments received.

On July 9, 2012, NIST published a notice in the Federal Register (77 FR 40338) announcing the Revised Draft FIPS 201-2 (''2012 Revised Draft''), which incorporated the changes from the 2011 Draft, based on the received public comments, and solicited comments on the revised draft standard. Comments and questions on the 2012 Revised Draft were submitted by 36 entities, composed of 16 U.S. federal government organizations, 19 private sector organizations, and one private individual. All comments received in response to both Federal Register notices have been made available by NIST at http://csrc.nist.gov. None of the commenters opposed the approval of a revised standard. Many commenters asked for clarification of the text of the standard and/or recommended editorial and/or formatting changes. Other commenters suggested modifying the requirements and asked questions concerning the implementation of the standard. All of the suggestions, questions, and recommendations within the scope of this FIPS were carefully reviewed, and changes were made to the standard, where appropriate. Some commenters submitted questions or raised issues that were related but outside the scope of this FIPS. Comments that were outside the scope of this FIPS, but that were within the scope of one of the related Special Publications, were deferred for later consideration in the context of the revisions to the Special

Publications. The disposition of each comment that was received has been provided along with the comments at http://csrc.nist.gov.

The following is a summary and analysis of the comments received during the public comment period, and NIST's responses to them, including the interests, concerns, recommendations, and issues considered in the development of FIPS 201-2:

Comment: Four commenters questioned the concept of backward compatibility as described in Section 1.3, Change Management, of the 2012 Revised Draft. They suggested that the Change Management section should not be restricted to the effects of changes to the Standard on PIV Cards but also address the effects of change to PIV systems and sub-components. Other commenters questioned whether any change to the Standard could be considered backward compatible.

Response: The Change Management section provides change management principles and guidelines to implementers of relying systems to manage newly introduced changes and modifications to the previous version of this Standard. In this context, changes to the Standard that do not necessitate changes to existing relying systems are considered to be backward compatible.

Comment: Two Federal agencies were concerned about their ability to implement the Standard with the indicated implementation schedule specified in the Standard.

Response: Issues concerning the Standard's implementation schedule have been referred to OMB.

Comment: Three commenters proposed that the procedures for PIV Card renewal and reissuance be combined.

Response: The Standard combines the two sections on PIV Card renewal and reissuance into one section called ‘‘Reissuance.’’ It addresses all instances in which a new PIV Card is issued to an existing cardholder without repeating the entire identity proofing and registration process.

Comment: Two commenters proposed adding a PIV-Interoperable (PIV-I) Card as a valid identity source document.

Response: The Standard does not list a PIV-I Card as an acceptable form of identity source documentation because it is not guaranteed to be a Federal or State government issued form of identification.

Comment: One commenter requested that the Standard prohibit the long-term storage of biometric data.

Response: FIPS 201-2 does not require the long-term storage of biometric data. However, PIV Card maintenance processes, such as reissuance, may be performed more efficiently if biometric data is maintained. Efficiency is a stated goal of HSPD-12.

Comment: The 2012 Revised Draft states that if the biometric data for the background investigation and the biometric data for the PIV Card are collected on separate occasions, then during the second visit, a one-to-one biometric match of the applicant must be performed against the biometric data

collected during the first visit. One commenter requested to remove the requirement for the one-to-one biometric match during the second visit, and that any requirements for one-to-one biometric matches begin after the biometric data for the PIV Card has been collected.

Response: In order to satisfy the control objectives of HSPD-12, it is necessary to verify that the biometric data for the background investigation was collected from the person to whom the PIV Card will be issued. A one-to-one biometric comparison is therefore required.

Comment: The 2012 Revised Draft imposes requirements to revoke the PIV Card under certain circumstances. Two commenters noted that the Standard should be more specific about the process for PIV Card revocation. One commenter also requested that the requirement to revoke the PIV Authentication and Card Authentication certificates during PIV Card termination be eliminated when the PIV Card is terminated for benign reasons.

Response: The text has been reorganized to clearly indicate the steps required to revoke a PIV Card. These steps include collecting and destroying the PIV card, if possible, and updating any databases maintained by the PIV Card issuer to reflect the change in status. Additionally, the requirements for certificate revocation during PIV Card termination have been relaxed. At PIV Card termination, revocation of the PIV Authentication and Card Authentication certificates is limited to cases where the PIV Card cannot be collected and destroyed.

Comment: One commenter indicated that a PIV derived credential on a mobile device should be revoked when the PIV Card's PIV Authentication certificate is revoked or expires.

Response: The PIV Authentication certificate on a PIV Card is revoked when the PIV Card is lost

or stolen. If the cardholder is eligible for a replacement PIV Card, the revocation of the derived credential would preclude the cardholder from using the derived credential to gain logical access to federally controlled information systems as an interim measure while waiting for a new PIV Card to be issued. Nothing in the Standard, however, prevents an agency from requiring its derived credential issuer to revoke a derived credential when the PIV Authentication certificate is revoked or expires.

Comment: The Standard includes a new feature to remotely reset the PIV Card's Personal Identification Number (PIN). One commenter suggested that the requirement to perform a biometric match as part of a remote PIN reset is too restrictive and should be removed.

Response: Removing the requirement to perform a biometric match from the remote PIN reset procedure would weaken the multi-factor authentication provided by the PIV Card. A biometric match is therefore required for all PIN reset procedures, regardless of whether the reset is performed in-person at an issuer's facility, at an unattended issuer-operated kiosk, or remotely from a general computing platform.

Comment: After publication of the Standard, SP 800-104, *A Scheme for PIV Visual Card Topography*, will be withdrawn, since all information of the Special Publication has been incorporated in the Standard. One commenter requested that the visual color scheme requirement from Special Publication 800-104, be made optional in FIPS 201-2 so that Federal departments and agencies with a need to distinguish between U.S. citizens and foreign nationals could use the color scheme on the PIV Card of their employees and contractors, while other Federal departments and

agencies without the need to visually distinguish between U.S. citizens and foreign nationals could issue PIV Cards without the distinction.

Response: The color scheme will remain mandatory in FIPS 201-2 because departments and agencies are required to accept PIV Cards issued by other Federal agencies, as directed by HSPD-12. Departments and agencies with a need to visually identify foreign nationals need the color scheme to be present on all PIV Cards, not just the PIV Cards that they issue.

Comment: Two commenters requested that a fourth category be added to the PIV Card's visual color scheme for employee affiliation or that the category for ''contractor'' be changed to ''non-government employee.''

Response: HSPD-12 establishes the scope for the Standard as "forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).'' With the scope established in HSPD-12, it would not be appropriate for the Standard to address employee affiliation color-codes other than employees and contractors.

Comment: Two commenters requested that the optional tactile markers on the PIV Card be more precisely defined.

Response: The two zones that are specified for tactile markers are intended to provide optional placement of orientation markers as a possible response to achieve Section 508 compliance. The implementation of tactile markers on PIV Cards should be coordinated with card manufacturers/vendors.

Comment: Three commenters expressed concern that the PIV Card's fingerprint reference data used for on-card biometric authentication and the PIV Card's fingerprint reference data used for off-card biometric authentication should not originate from the same anatomical fingers. The commenters noted that an attacker may maliciously obtain the PIV Card's fingerprint reference data during an off-card biometric authentication event. With the harvested reference data and with a malware injected computing platform, other attacks can be staged to target applications that use the on-card authentication mechanisms.

Response: Section 4.4.4 of the Standard stresses the need for general good practices to mitigate malicious code threats. In addition to general good practice, the Standard allows the fingerprint reference data to originate from a different finger. Additionally, NIST Special Publication 800-76-2 will clarify the usability versus security trade off associated with a possible confusion about which finger to present at an authentication event.

Comment: Four commenters noted that 2012 Revised Draft allows for use of the electronic facial image as an option for authentication in operator-attended PIV Card issuance and reissuance processes but does not extend its use as an authentication mechanism in physical access control environments.

Response: Comparison of electronic facial images depends on carefully controlled environments with controls to camera height and lighting. These controls are not consistently found in general purpose physical access control environments. This Standard therefore limits facial recognition as a cost-efficient and optional authentication mechanism for PIV Card issuance, reissuance and

verification data reset processes where the environment is controllable. FIPS 201-2 offers fingerprint biometric and iris recognition for general-purpose physical access control environments, as both mechanisms provide better accuracy, security, and speed.

Comment: Technical issues were raised by three commenters concerning the need for a person identifier to be present on the PIV Card. The commenters stated that without a person identifier, access control systems are required to re-provision cardholders each time a cardholder replaces his or her card. A person identifier, however, alleviates re-provisioning by providing a persistent identifier for the access control systems to recognize a cardholder with a new PIV Card.

Response: An optional person identifier will be proposed in the Standard's associated publication, Special Publication 800-73.

Comment: Issues were raised by two commenters about the PIV Card's cryptographic keys that are used in authentication and digital signatures. The commenters pointed out that a PIV Card issuer should have the flexibility to generate the PIV Authentication key, the Card Authentication key, and Digital Signature key off-card.

Response: Because the authentication mechanism used with the asymmetric Card Authentication key provides only some confidence in the cardholder's identity, off-card generation and import of this key, is allowed by the Standard. For the PIV Authentication key and Digital Signature key, however, on-card generation of the keys remains a requirement because an off-card generation of these keys adversely affects the perceived level of assurance in the cardholder's identity.

Comment: Three commenters requested that the PIV Card's secure messaging feature and its virtual contact interface be made mandatory as soon as possible for the many beneficial features that they enable.

Response: While there has been significant demand for the inclusion of secure messaging and the virtual contact interface in the Standard, some Federal departments and agencies have expressed concerns about the risks of adopting this technology. Therefore, it is appropriate to allow individual agencies to make a risk-based decision as to whether to include these technologies in their PIV Cards.

Comment: Two commenters requested that specific requirements for the public key infrastructure (PKI) be addressed in the ''X.509 Certificate Policy For The U.S. Federal Common Policy Framework'' rather than in the Standard, in order to allow for the requirements to be modified to accommodate new and emerging technologies.

Response: As the scope of the Common Policy is not limited to PIV Cards, the Standard needs to include information about which certificate policies may be used to issue the different types of certificates needed for PIV Cards, as well as other PIV-specific information. Care has been taken to ensure that any PKI-related requirements specified in FIPS 201-2 are unlikely to change before the next revision of the Standard.

Comment: Three commenters requested that the Standard either allow or require the use of a content signing-specific certificate policy Object Identifier (OID) in certificates issued to entities that sign data objects on PIV Cards.

Response: Sections 4.2.1 and 4.2.3.2 now require that after a transition period, certificates used to sign data objects on PIV Cards shall assert a content signing-specific policy OID from the ‘‘X.509 Certificate Policy For The U.S. Federal Common Policy Framework.’’

Comment: Three commenters noted that the 2012 Revised Draft describes authentication mechanisms that utilize the PIV Card and requested that the Standard indicate that agencies may choose to use other authentication mechanisms that are not applicable to the Standard.

Response: OMB has oversight of agency implementation of the Standard. Thus, it is not suitable for FIPS 201–2 to indicate that agencies are permitted to implement authentication mechanisms other than those described in FIPS 201–2.

Comment: The 2012 Revised Draft lowers the assurance level of the Cardholder Unique Identifier (CHUID) authentication mechanism from some confidence in the identity of the cardholder to little or no confidence, and deprecates its use. Two commenters indicated that Federal departments and agencies have been working to enable their physical access control systems to use the CHUID authentication mechanism and suggested that the authentication mechanism should continue to be described as providing some confidence, and its use should not be deprecated.

Response: In order for an authentication mechanism to provide some confidence in the identity of the cardholder, it would have to align with the requirements comparable to those specified for E-Authentication Level 2 of NIST Special Publication 800-63-1. The CHUID authentication mechanism does not satisfy these requirements. It is, therefore, appropriate to describe the authentication mechanism as providing little or no confidence in the identity of the cardholder and

to deprecate its use in authentication events.

Revised FIPS 201-2 is available electronically from the NIST web site at:

http://csrc.nist.gov/publications/PubsFIPS.html

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, 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 the purposes of E.O. 12866.

Dated: August 28, 2013

Willie E. May
Associate Director for Laboratory Programs

[FR Doc. 2013-21491 Filed 09/04/2013 at 8:45 am; Publication Date: 09/05/2013]