Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

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

[Docket No.: 120608158-2158-01]

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

ACTION: Notice and request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) announces the Revised Draft Federal Information Processing Standard (FIPS) Publication 201–2, ‘‘Personal Identity Verification of Federal Employees and Contractors,’’ for public review and comment. The draft standard, designated ‘‘Revised Draft FIPS 201–2,’’ is proposed to supersede FIPS 201–1. NIST will hold a public workshop at NIST in Gaithersburg, Maryland, to present the Revised Draft FIPS 201–2. Please see admittance instructions in the SUPPLEMENTARY INFORMATION section below.

DATES: Comments must be received by Friday, August 10, 2012. The public workshop will be held on Wednesday, July 25, 2012. Preregistration must be completed by 5:00 PM Eastern Time on Wednesday, July 18, 2012.

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, ATTN: Comments on Revised Draft FIPS 201–2, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930. Electronic comments may be sent to: piv_comments@nist.gov. Anyone wishing to attend the workshop in person, must pre-register at http://www.nist.gov/allevents.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: 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, email: david.cooper@nist.gov.

SUPPLEMENTARY INFORMATION: FIPS 201 was issued on April 8, 2005 (70 FR 17975), and in accordance with NIST policy was due for review in 2010. In consideration of technological advancement 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 Office of Management and Budget (OMB) and USG stakeholders, were incorporated in the Draft FIPS 201–2.

Other change requests incorporated in the Draft FIPS 201–2 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 a proposed revision of FIPS 201–1 (hereafter referred to as 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. NIST developed the Revised Draft FIPS 201–2 that is announced in this notice using the comments received in response to the March 8, 2011, notice.

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. These comments have all been made available by NIST at http://csrc.nist.gov. None of the commenters opposed the approval of a revised standard. Some commenters asked for clarification of the text of the standard and/or recommended editorial and/or formatting changes. Other commenters suggested modifying the requirements. 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 supporting 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:

*Comment*: Seven commenters stated that the document should be reorganized since it includes logical card characteristics in the section on physical card characteristics and it does not describe the requirements for the collection of biometric data until long after references to the biometric data are first made.

*Response*: Requirements for the collection of biometric data and recommendations for the maintenance of a chain-of-trust have been moved from Section 4 to the beginning of Section 2. Section 4 has also been reorganized to separate the requirements for the logical card characteristics from the requirements for the physical card characteristics.

*Comment*: The 2011 Draft proposed a secure messaging capability. Six commenters indicated that the proposed secure messaging capability needs to be enhanced in order to permit all functionality of the PIV Card to be accessible over the contactless interface of the card.

*Response*: The Revised Draft FIPS 201–2 introduces the concept of a *virtual contact interface*, over which all functionality of the PIV Card is accessible.

*Comment*: Seven commenters indicated that the standard needs to accommodate the Federal Government's movement towards mobile devices and permit the issuance of PIV Cards that have form factors other than the current International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 (credit-card) form factor.

*Response*: The Revised Draft FIPS 201–2 continues to require every cardholder to be issued an ISO/IEC 7810 form factor PIV Card, but it introduces the ability to issue PIV derived credentials, which may be provisioned to devices other than an ISO/IEC 7810 form factor.

*Comment*: The 2011 Draft introduced iris images as an alternative to fingerprints for individuals from whom fingerprints cannot be collected. Three commenters suggested that the use of iris as an alternative is an undue burden. Six commenters noted that the 2011 Draft is unclear about how to address applicants from whom neither fingerprints nor iris images can be obtained.

*Response*: The Revised Draft FIPS 201–2 makes collection of iris images optional. During PIV Card issuance and maintenance processes a one-to-one biometric match is required. However, the Revised Draft FIPS 201–2 permits the use of automated iris or facial image matching when fingerprints are unavailable. In cases where iris or facial image data is not available or where the issuer does not support automated biometric comparison based on these types of biometrics, identity source documents may be used to verify the identity of the applicant or cardholder.

*Comment*: Twelve comments addressed the Lightweight Directory Access Protocol (LDAP) as a means to distribute certificates and Certificate Revocation Lists (CRLs). These comments indicated that LDAP is not used and the Hypertext Transfer Protocol (HTTP) is now considered the preferred option to distribute certificates and Certificate Revocation Lists (CRLs).

*Response*: The Revised Draft FIPS 201–2 removes the requirement to distribute certificates and CRLs via LDAP, but continues to require conformance to the ‘‘X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program,’’ which can be updated as necessary to account for changes in technology.

*Comment*: Ten comments indicated that the requirements for issuing PIV Cards to applicants during the grace period are unclear and appear to conflict with guidance from the Office of Personnel Management (OPM) with respect to requirements for background re-investigations.

*Response*: The section describing the grace period has been rewritten to clarify the requirements and to make it clear that background re-investigations only need to be performed if required, in accordance with OPM guidance.

*Comment*: Twelve commenters noted that the difference between reissuance and renewal of PIV Cards is unclear.

*Response*: The Revised Draft FIPS 201–2 indicates that PIV Card renewal applies when a valid PIV Card is replaced with a new card and that PIV Card reissuance applies when a new PIV Card is issued to replace a lost, stolen, or damaged card. PIV Card reissuance also applies when a card is replaced because one or more of its logical credentials have been compromised.

*Comment*: Four commenters indicated that Federal agencies should be able to perform Personal Identification Number (PIN) resets without requiring cardholders to appear in person before a card issuer. It is unclear whether remote resets are permitted in the 2011 Draft.

*Response*: The requirements for resetting PINs have been rewritten in the Revised Draft FIPS 201–2. The Revised Draft FIPS 201–2 specifies different requirements for resetting a PIN depending on whether the PIN is reset in-person at an issuer's facility, at an unattended issuer-operated kiosk, or remotely from a general computing platform (e.g., desktop or laptop).

*Comment*: FIPS 201–1 and the 2011 Draft describe two very weak authentication mechanisms as providing some assurance in the identity of the cardholder: visual inspection of the PIV Card by a human guard (VIS) and reading the cardholder unique identifier from the card (CHUID). Fifteen comments were received about the CHUID and VIS authentication mechanisms indicating that the use of these two authentication mechanisms should be deprecated.

*Response*: The Revised Draft FIPS 201–2 states that the VIS and CHUID authentication mechanisms provide little or no assurance in the identity of the cardholder. The Revised Draft FIPS 201–2 also deprecates the use of the CHUID authentication mechanism.

*Comment*: The 2011 Draft defines some authentication mechanisms that may be difficult or impossible for individuals with certain disabilities to perform. Three commenters noted that the 2011 Draft does not clearly indicate what departments and agencies need to do to accommodate individuals with disabilities.

*Response*: The processes for issuing, reissuing, renewing, and resetting PIV Cards have been updated to include new options for authenticating the cardholder in the case that authentication cannot be performed using a match of either fingerprints or iris images. While Revised Draft FIPS 201–2 describes authentication mechanisms that can be implemented using the PIV Card, which may be used to authenticate individuals who are attempting to gain physical access to federally controlled facilities or logical access to federally controlled information systems, it is the responsibility of departments and agencies developing access control systems to choose the authentication mechanisms that are appropriate for their systems. The Revised Draft FIPS 201–2 includes a reminder to departments and agencies that when implementing PIV systems they should consider provisions to accommodate employees and contractors with disabilities in accordance with Section 508 of the Rehabilitation Act.

*Comment*: Information about card topography is currently split between the 2011 Draft and NIST Special Publication 800–104, *A Scheme for PIV Visual Card Topography*. Three commenters noted that it would be clearer if all of this information is consolidated in one document.

*Response*: All of the information from Special Publication 800–104 has been incorporated into the Revised Draft FIPS 201–2, and Special Publication 800–104 will be withdrawn after FIPS 201–2 has been approved. As a result of incorporating Special Publication 800–104 into Revised Draft FIPS 201–2, the employee affiliation color-coding and the large expiration date in the upper right-hand corner of the card are now mandatory. Revised Draft FIPS 201–2 also now states that the ''Federal Emergency Response Official'' indicator or country of citizenship information, when present, shall be indicated at the bottom of the card.

*Comment*: Three commenters noted that there is no information on adoption/migration between versions of FIPS 201 and that guidance is needed to distinguish which version of FIPS 201 was used to issue a given card. Seven commenters also pointed out that guidance is needed on the adoption/migration of new features.

*Response*: The version management for PIV Cards and middleware will be addressed in revisions to Special Publication 800-73, *Interfaces for Personal Identity Verification*. New features of FIPS 201–2 that depend upon the release of new or revised NIST Special Publications are effective immediately upon final publication of the supporting Special Publication. A timetable to achieve compliance with FIPS 201–2 has been coordinated with OMB and is included in the Revised Draft FIPS 201-2.

*Comment*: One commenter noted that the chain-of-trust introduces a new requirement that is cost-prohibitive to implement.

*Response*: The chain-of-trust is optional in the Revised Draft FIPS 201–2. The concept of chain-of-trust was requested by federal agencies as a cost savings measure that streamlines current practices for issuance, reissuance, and renewal procedures. Agencies can use their internally defined enrollment data records as the means to implement the chain-of-trust. The Revised Draft FIPS 201–2 only requires specific formats and structures for the import and export of chain-of-trust records for agencies choosing to implement interagency transfer of enrollment data records.

*Comment*: Six commenters noted that it is unclear what type of data is part of the chain-of-trust records.

*Response*: In the Revised Draft FIPS 201–2, the section describing the chain-of-trust includes recommendations for the type of data to be collected and included in the chain-of-trust.

*Comment*: Five commenters noted that in addition to printing the facial image on the card, most issuers today also store the facial image electronically in the chip on the card. FIPS 201–2 should make this mandatory in order to provide a low cost alternative for cardholder identification and authentication.

*Response*: As requested by federal agencies, Revised Draft FIPS 201–2 defines the facial image as part of HSPD-12 ''common identification'' credential by including it as one of the core mandatory logical credentials of the PIV Card. The digital signature key and key management key are also included as core mandatory credentials of the PIV card. These additional changes were requested by OMB in order to align the Revised Draft FIPS 201-2 with the *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*.

*Comment*: Seven commenters requested that the Universally Unique Identifier (UUID) be made mandatory for interoperability between PIV and PIV–Interoperable (PIV–I) ecosystems.

*Response*: In response to the many similar comments, the Revised Draft FIPS 201–2 specifies the UUID as a mandatory unique identifier for the PIV Card, in addition to the Federal Agency Smart Credential Number (FASC-N).

*Comment*: Many federal employees and contractors prefer to be known by a professional name that is different from the name used in personal lives. Three commenters requested that FIPS 201–2 permit the cardholder's professional name to be printed on the PIV Card rather than the name appearing on the cardholder's identity source documents.

*Response*: NIST raised this issue with OMB, which is responsible for making decisions on this type of issue. Because the PIV card is an official USG issued card, OMB determined that the name that appears on the PIV Card must be the name that has been verified through identity source documents.

Comment: One commenter requested that the Revised Draft FIPS 201-2 should reaffirm that PIV Card Issuers' self-accreditation as specified in SP 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers,* remains in effect.

Response: The Revised Draft FIPS 201-2 clarifies that self-accreditation as per SP 800-79 continues to be acceptable, so long as it is supplemented by a third-party accreditation review.

*Comment*: Three commenters stated that requiring a biometric match between the full set of fingerprints collected for law enforcement checks and the two fingerprints collected for placement on the PIV Card is an undue burden since these two sets of fingerprints are commonly collected on two

different systems that are not integrated.

*Response*: The Revised Draft FIPS 201–2 makes it clear that a biometric match is only required if the two sets of fingerprints are collected on separate occasions, and is not required if the two sets are collected at the same time on different systems. The Revised Draft FIPS 201–2 also clarifies that a full set of fingerprints does not need to be collected from an applicant if a completed and favorably adjudicated National Agency Check with Written Inquiries (NACI) (or equivalent or higher) or Tier 1 or higher federal background investigation can be located and referenced for the individual.

*Comment*: Four commenters noted that Federal agencies should be permitted to register PIV–Interoperable (PIV-I) credentials in lieu of issuing PIV credentials provided that attributes such as successful completion of a NACI can be electronically validated.

*Response*: HSPD–12 specifies that agencies shall use ''secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).'' The use of an externally issued credential, such as a PIV–I credential, as an alternative to issuing a PIV Card, would not be consistent with HSPD-12.

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

Public Workshop: NIST will hold a public workshop on Revised Draft FIPS 201–2 on Wednesday, July 25, 2012, 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/allevents.cfm by 5:00 PM Eastern Time on July 18, 2012, in order to enter the NIST facility and attend the workshop.

Authority: 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 to be not significant for purposes of E.O. 12866.

Dated: July 2, 2012

Willie E. May
Associate Director for Laboratory Programs

[FR Doc. 2012-16725 Filed 07/06/2012 at 8:45 am; Publication Date: 07/09/2012]