Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. [201023-0280]

Request for Comments on Federal Information Processing Standard (FIPS) 201-3

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

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) requests comments on Draft Federal Information Processing Standard (FIPS) 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (Standard). This Standard defines common credentials and authentication mechanisms offering varying degrees of security for both logical and physical access applications. The draft revision proposes changes to FIPS 201-2, Standard for Personal Identity Verification of Federal Employees and Contractors to include: expanding specification on the use of additional PIV credentials known as derived PIV credentials, procedures for supervised remote identity proofing, the use of federation as a means for a relying system to interoperate with PIV credentials issued by other agencies, alignment with the current practice/policy of the Federal Government and specific changes requested by Federal agencies and implementers. Before recommending these proposed changes to the Secretary of Commerce for review and approval, NIST invites comments from all interested parties.

DATES: Comments on FIPS 201-3 must be received on or before [INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: The draft of FIPS 201-3 is available for review and comment on the NIST Computer Security Resource Center website at *https://csrc.nist.gov* and at *https://www.regulations.gov/.* Comments on FIPS 201-3 may be sent electronically to *piv_comments@nist.gov* with "Comment on FIPS 201-3" in the subject line or may be submitted via *https://www.regulations.gov/*. Comments may also be submitted on the project repository at *https://github.com/usnistgov/FIPS201*. Written comments may be submitted by mail to Information Technology Laboratory, ATTN: FIPS 201-3 Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930.

All submissions, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. NIST reserves the right to publish relevant comments, unedited and in their entirety. Relevant comments received by the deadline will be published electronically at *https://csrc.nist.gov/* , *https://www.regulations.gov/* and the project repository at *https://github.com/usnistgov/FIPS201* without change or redaction, so commenters should not include information they do not wish to be posted. Personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Do not submit confidential business information or otherwise sensitive or protected information. Comments that contain profanity, vulgarity, threats, or other

inappropriate language or content will not be posted or considered.

FOR FURTHER INFORMATION CONTACT: Hildegard Ferraiolo, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop Number 8930, Gaithersburg, MD 20899-8930, email: hferraio@nist.gov, phone: (301) 975-6972.

SUPPLEMENTARY INFORMATION:

FIPS 201 defines common credentials and authentication mechanisms offering varying degrees of security for both logical and physical access applications. Federal departments and agencies will determine the level of security and authentication mechanisms appropriate for their respective applications. The scope of this Standard is limited to authentication of an individual's identity. Authorization and access control decisions are outside the scope of this Standard. Moreover, requirements for a temporary credential used until a new or replacement PIV credential arrives are out of scope of this Standard.

In accordance with NIST policy, FIPS 201-2 (the version of the Standard currently in effect) was due for review in 2018. In consideration of changes in the environment over the last several years and of specific requests for changes from Federal agencies, NIST determined that a revision of FIPS 201-2 is warranted. NIST has received numerous change requests, some of which, after analysis and coordination with the Office of Management and Budget (OMB), the Office of Personnel Management (OPM), and other Federal agencies, are incorporated in the Draft FIPS 201-3. Other change requests incorporated in the Draft FIPS 201-3 result from the 2019 Business Requirements

Meeting held at NIST. The meeting focused on business requirements of Federal agencies. The proposed changes in Draft FIPS 201-3 are:

- Alignment with SP 800-63-3 language and terms.
- Updated OMB policy guidelines references from rescinded OMB memorandum M-04-04 to new guidelines in OMB memorandum M-19-17.
- Updated process for binding and termination of derived PIV credentials with PIV account.
- Updated credentialing requirements for issuance of PIV Cards based on OPM guidance.
- Added requirements for supervised remote identity proofing and PIV Card maintenance.
- Modified identity proofing requirements to reflect updated list of accepted documents.
- Updated guidance on validation of identity proofing documents.
- Updated guidance on collection of biometric data for credentialing.
- Clarified multi-session proofing and enrollment.
- Clarified biometric modalities for proofing and authentication.
- Provided clarification on grace periods.
- Deprecated PIV National Agency Check with Written Inquiries (NACI) indicator (background investigation indicator).
- Updated system description and associated diagrams.
- Generalized chain of trust records to enrollment records and made these records required.

- Deprecated the use of magnetic stripes and bar codes on PIV Cards.
- Linked expiration of content signing certificate with card authentication certificate.
- Revised PIN requirements based on SP 800-63B guidelines.
- Removed requirement for support of legacy PKIs.
- Expressed authentication assurance levels in terms of Physical Assurance Level (PAL) and Authenticator Assurance Level (AAL).
- Removed previously deprecated Cardholder Unique Identifier (CHUID) authentication mechanisms. The CHUID data element has not been deprecated and continues to be mandatory.
- Deprecated symmetric card authentication key and associated authentication mechanism (SYM-CAK).
- Added support for secure messaging authentication mechanism (SM-AUTH).
- Deprecated visual authentication mechanism (VIS).
- Added section discussing federation in relationship to PIV credentials.

A public workshop will be held for FIPS 201-3. The specific date will be determined and posted on the NIST Personal Identity Verification (PIV) website: https://csrc.nist.gov/Projects/PIV. Before recommending these proposed changes to the Secretary of Commerce for review and approval, NIST invites comments from all interested parties.

Authority: 44 U.S.C. 3553(f)(1), 15 U.S.C. 278g-3.

Kevin Kimball,
Chief of Staff.

[FR Doc. 2020-24283 Filed: 11/2/2020 8:45 am; Publication Date: 11/3/2020]