X-Sieve: CMU Sieve 2.2
From: "Mayhle, Art" <Art.Mayhle@ssa.gov>
To: "'draftfips201@nist.gov'" <draftfips201@nist.gov>
Cc: ^OCIO Controls <OCIO.Controls@ssa.gov>,
"Hughes, Tom CIO"
<Tom.Hughes@ssa.gov>,
"Barsczewski, Gerry" <Gerry.Barsczewski@ssa.gov>
Date: Thu, 23 Dec 2004 13:07:50 -0500
Importance: high
X-Mailer: Internet Mail Service (5.5.2657.72)
X-MailScanner:
X-MailScanner-From: art.mayhle@ssa.gov
Subject: Social Security Response for CIOCL Request for Comments on Draft

"urn:schemas-microsoft-com:office:office">
Attached find the Social Security Administration's comments on the draft NIST Identity Standard. Questions may be directed to me.

Art Mayhle, CISSP, CISM

Chief Security Officer

Social Security Administration

Office of the Chief Information Officer

6401 Security Blvd.

Room 500

VOICE (410) 965-2823

FAX (410) 966-2805

Art.Mayhle@ssa.gov

-----Original Message-----
From: CIO-COUNCIL [mailto:CIO-COUNCIL@listserv.gsa.gov] **On Behalf Of** Edward Roback
Sent: Tuesday, November 09, 2004 8:07 AM
To: CIO-COUNCIL@listserv.gsa.gov
Subject: [CIOCL] Draft NIST Identity Standard

MEMORANDUM FOR Members of the Federal CIO Council

From: Ed Roback,
Chief, NIST Computer Security Division

1. Draft Standard -- Personal Identification Verification for Federal Employees and Contractors

Under Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, the President has directed the development of a Federal standard for secure and reliable forms of identification.

NIST has developed the draft (mandatory) standard, which is now available for public review and comment. This Federal Information Processing Standard (FIPS), *Personal Identity Verification (PIV) for Federal Employees and Contractors*, was developed in the context of a number of diverse Federal access credential standardization and implementation programs. The draft was prepared with many valuable inputs from the Federal Technical Interagency Working group. It is available at http://csrc.nist.gov/publications/drafts.html .

The standard is comprised of two parts. Part I includes control objectives derived from HSPD #12 and an identity proofing process structured to satisfy the intent of HSPD #12 and provide for reciprocity. Part 2 includes detailed specifications intended to support technical interoperability among Federal departments and agencies. In compliance with HSPD #12, Part I must be implemented no later than eight (8) months following promulgation of FIPS #201 (PIV). Agency implementation of Part 2 will be accomplished in accordance with implementation guidance to be developed by the Office of Management and Budget.

Comments are requested by December 23, 2004 so that we may meet the President's deadline for completing the standard. A single, consolidated/consistent set of comments from each agency with comments would be greatly appreciated. Comments may be sent to: draftfips201@nist.gov .

2. Draft Security Guideline

Along with the draft standard, Draft NIST Special Publication 800-73, *Integrated Circuit Card for Personal Identification Verification*, is being made available for public review. Special Pub 800-73 defines the interoperable card platform for the PIV framework (specified in the draft PIV standard.) This platform is derived from the existing Government Smart Card Interoperability Specification, Version 2.1 (NISTIR 6887), and relevant international smart card standards. The draft guideline is available at http://csrc.nist.gov/publications/drafts.html .


Consolidated FIPS 201 Comments 12-23-04.doc

Social Security Administration
Comments on Draft FIPS PUB 201
"Personal Identity Verification Standard"

General Comments

As stated in our previous comments, full compliance with FIPS 201 will cost SSA $30-35 million in upfront costs for both physical and logical access components. In subsequent years, ongoing maintenance costs will be $3-5 million. SSA's enacted appropriation for FY 2005 and budget request for FY 2006 to OMB will not permit SSA to meet the full requirements in PIV-I. Implementation presents logistical problems for issuing credentials to our 105,000 employees, contractors, and trusted partners around the country. Most of our employees, contractors, and trusted partners do not currently possess a government ID. The first opportunity to budget for all the costs associated with both portions of FIPS 201 will be in FY 2007, and OMB will need to factor this activity into their planning and implementation guidance.

Specific Comments

Item 1
Reference: Page 4. Section 2.1 Control Objectives
Issue: Agencies are to issue identity credentials that are resistant to fraud, tampering, counterfeiting and terrorist exploitation.
Comment: The remainder of the section on PIV-I does not contain specific requirements for the credentials issued under the initial portion of the standard.

Item 2
Reference: Page 5. Section 2.2.1 Identity Proofing and Registration of New Employees and Contractors
Issue: The Registration Authority fingerprints applicants.
Comment: We suggest making a statement that fingerprints must be taken by a trusted source and that the Agency has the necessary controls in place to ensure compliance (e.g., local police).

Item 3
Reference: Page 14. Section 3.3.2 PIV Card Issuance and Management Subsystem
Issue: All of the applicant registration data collected at the onset of the registration process, including the biometric data as well as any updates to this information during the usage of this card, is stored in the Registration Repository.
Comment: If the biometric/photo/signature/personal information is stored on any database, the information should be held in separate databases to ensure that the compromise of one database would not compromise all information on any one individual.

Item 4
Reference: Page 30. Section 4.4 Biometric Specifications
Issue: An electronic facial image will be stored on the card for an alternate identity verification process.
Comment: While facial imaging is needed in order to be 508 compliant mandating the use of a facial image as an alternative to using two index fingers will drive up costs. To use this feature, entry portals at every building will need the equipment and software required for this process. Given the small percentage of individuals involved, agencies should retain the authority to decide whether or not facial imaging is necessary and should be allowed to make these determinations on a case by case basis.

Item: 5
Reference: Page 46. 5.2.4.2 Re-Issuance
Issue: In case of re-issuance, a new personalization, including fingerprint and facial image capture, shall be conducted.
Comment: In the case of a trusted government employee, agencies should be allowed to issue a temporary card while the new permanent card is being processed.

Item: 6
Reference: Page 47. 5.2.4.2 Re-Issuance
Issue: Where the card cannot be collected, normal operational procedures shall complete within 18 hours of notification. In some cases, 18 hours is an unacceptable delay. In such a case, emergency procedures must be executed to disseminate this information as rapidly as possible. Agencies are required to have procedures in place to update all servers in one hour in the case of such an emergency.
Comment: More clarification on the notification aspect of the statement is required. Updating all servers (and thus, all access portals for buildings) within one hour's notice may not be realistic for an agency with a global infrastructure.

Item 7
Reference: Page 53. 6.1.5 Authentication using PIV Asymmetric Cryptography
Issue: The reader issues a challenge string to the card and requests an asymmetric operation in response.
Comment: The card should have a way of also authenticating that the reader is who it says it is in a system of cross-authentication. Not only should readers not accept interfacing with false cards, but also cards should not accept interfacing with false readers.

Item 8
Reference: Page 54. 6.2.1 Assumptions and Constraints
Issue: Physical access control systems tend to rely heavily upon offline or out-of-band means of pre-approving a cardholder for access to a particular secure site.
Comment: To the contrary, many of SSA's physical entry points at larger facilities have personal computers connected to LAN applications. The long-range implications of

PIV-II are that physical access portals to higher security sites need to be connected to the automated access system in order to control entry of individuals to these secure sites. This will be facility specific depending upon the security level for each facility as determined by each agency, but agencies should be planning for LAN connections at physical entry portals for higher security locations and where it makes operational sense.

Item 9
Reference: Page 57. Section 6.3 - Authentication for Logical Access Control
Issue: The PIV card may be used to authenticate the cardholder in support of access control decisions for information resources. For example, a cardholder may login to their agency network using the PIV card. The identity established through this authentication process can be used for determining access to file systems, databases, and other services available on the network.
Comment: We would like to see additional clarification regarding when the card will be needed for logical access. What impact, if any, do the Assurance Levels outlined in Appendix B.2 "Logical Access Support" have upon the decision to apply PIV authentication to a given logical resource?