From: William Barker [wbarker@nist.gov]
Sent: Tuesday, December 21, 2004 3:06 PM
To: Mehta Ketan; grance@nist.gov; branstad@nist.gov
Subject: Fwd: Comments on FIPS 201

Attachments: Policy Overview.doc

Policy
Overview.doc (69 KB

>X-Sieve: CMU Sieve 2.2
>From: Helena Sims <HSIMS@NACHA.ORG>
>To: "'cbarker@nist.gov'" <cbarker@nist.gov>
>Cc: "'wbarker@nist.gov'" <wbarker@nist.gov>
>Subject: Comments on FIPS 201
>Date: Tue, 21 Dec 2004 13:36:11 -0500
>X-Mailer: Internet Mail Service (5.5.2653.19)
>X-OriginalArrivalTime: 21 Dec 2004 18:28:15.0375 (UTC)
>FILETIME=[D5EC41F0:01C4E78A]
>X-MailScanner:
>X-MailScanner-From: hsims@nacha.org
>
>As follow-up to the meeting that representatives from the Federation
>for Identity and Cross-Credentialing Systems (FiXs) recently had with
>NIST representatives on December 10, 2004, I am writing to provide you
>with supplementary information that you requested on FIPS 201 and
>related guidance. Specifically, we were asked to break recommended
>requirements into policy and technical guidance. Thank you for taking
>the time to meet with us on the 10th. We appreciate the opportunity to
>talk with you and your colleagues from NIST.
>
>Comments on FIPS PUB 201
>
>Homeland Security Presidential Decision (HSPD)-12 directed the Commerce
>Department to promulgate a mandatory, Government-wide standard for
>secure and reliable forms of identification issued by the Federal Government to its
>employees and contractors (including contractor employees).   FIPS 201 is
>the critical technical component of this process. However, because of
>its very technical nature, FIPS 201 by itself is not sufficient to
>provide a Government-wide framework for secure and reliable forms of identification.
>In addition, guidance that also mandates an overarching government
>policy is required. The recommended overarching guidance, presented in
>order of the most high-level policy documents to the most specific
>implementation requirements, are:
>
>*   A Trust Statement,
>*   A Policy Statement,
>*   Operating Rules,
>*   Technical Requirements (contained in FIPS 201, et al), and
>*   Memoranda of Understanding.
>
>Copies of these documents for the FiXs program can be accessed at
>www.FiXs.org. They were also included in FiXs comment letter on
>HSPD-12, dated October 21, 2004.
>
>FiXs actively participates in PIV development under the Interagency
>Advisory Board's Working Group (IABAWG -Technical). We support the
>intent of the NIST work taking form in FIPS 201 and its supporting
>documentation, especially SP 8000-73. Again, while we note that FIPS

>201 is an essential element of a framework for establishing a
>mandatory, Government-wide standard for secure and reliable forms of
>identification, we maintain that, by itself, the FIPS is an incomplete response to the
intent of HSPD-12.
>
>The recommended overarching guidance addresses a number of key
>elements,
>including: a standard policy on person-proofing; a standard method of
>secure enrollment, a standard method of card and person management, a
>finite list of compliance criteria, an independent assessment method,
>and strict enforcement processes. We suggest a major heading outline
>for the recommended guidance in attachment to this document entitled
>"Policy Overview."
>
>We are available to assist you in developing the important policy and
>process necessary to the success of PIV. Our point of contact for this
>effort is Dr. Michael Mestrovich at (703) 730-3556. I can be reached
>at (703)561-3930.
>
>About FiXs
>
>FiXs was established to implement a federated identity management and
>cross-credentialing program between the Department of Defense (DoD) and
>defense contractors. Its objective is to create a federated network to
>support interoperable use and authentication of identity credentials.
>
>FiXs is currently supporting two segments of this evolving federated
>identity infrastructure: 1) DoD's system, known as the Defense
>Cross-Credentialing Identification System (DCCIS), as a part of their
>Defense National Visitor's Center (DNVC) application, and 2) the
>non-DoD government and private sector system known as the FiXs system.
>
>The FiXs Federation enables participating DoD facilities to achieve
>strong and interoperable identity verification and authentication of
>contractors/private sector employees participating in the FiXs system.
>Contractors and private sector employers can verify and authenticate
>other industry, federal and DoD employees at facilities participating
>in the FiXs and DCCIS Network. As additional organizations join the
>program, they will be able to participate by agreeing to comply with
>the FiXs Federation policies and operating rules.
>
> <<Policy Overview.doc>>
>
>
>
>
>
>