

Mehta Ketan

From: Mark Lombard [MXL7@nrc.gov]
Sent: Thursday, December 23, 2004 4:22 PM
To: DraftFips201@nist.gov
Cc: Wbarker@nist.gov; Cynthia Harbaugh; Elizabeth Langley; Kathy Lyons-Burke; Patricia Smith; Susan Cusseaux; Sandra Schoenmann; Thomas Martin
Subject: NRC comments on draft NIST publications for HSPD-12

The following are the Nuclear Regulatory Commission (NRC) comments on the draft NIST publications to implement HSPD-12. Please contact me if you have any questions.

FIPS PUB 201

* General: The standard implies that each individual who has access to an agency's facility will be processed and issued a unique card. It is our experience that for the number of individuals that have only a short-term or infrequent need for access, this requirement would be cost prohibitive and create accountability issues with respect to the card.

* General: The standard refers to card expiration dates in several places. Printing cards with an expiration date on it would be cost prohibitive. The card should interface with the home agency system and be "smart" enough to identify a terminated or expired card.

* General: The standard does not address Privacy Act or System of Records requirements associated with the information collected and stored on the card.

* General: The standard does not address specific requirements that need to be incorporated into existing or future agency contracts.

* Page 21, Section 4.1, first paragraph, second sentence: This sentence contradicts itself. Cards can't both "interoperate with access control systems across agencies" and also enable "agencies to make access control decisions." The first phrase indicates the access control system will allow access (i.e., open the gate) if the card carrier is authorized for access to that facility but the second phrase indicates the other agency still will make the access control call and/or issue additional access control media.

* Page 21, Section 4.1, last paragraph: Will the final standard how to handle lost or forgotten badges?

* Section 5.1: The NRC is very appreciative that NIST heard our, and other agency's, concerns and deleted the requirements for background investigations based on the DOJ facility security levels. The revised wording is logical and realistic.

* Sections 6.5.1.2 and 6.5.2.2: NRC's OGC required us to also list Section 701 Title 18 of the US Code on the back of our cards.

NIST Special Publication 800-XX, Version 0.1

No NRC comments.

Mark Lombard
Chief, Security Branch
U.S. Nuclear Regulatory Commission
301-415-7404
240-375-7623-cell
301-415-5132-fax