NIST Comments on OMB Draft HSPD#12 Implementation Guidance
==========

Section 1. Define or recommend a definition for "long-term access." Currently, agencies are having to define what "long term" is. It would be helpful (and consistent) if OMB were to recommend a definition for it.

Section 1.B. Define or recommend "short-term access" to be consistent across federal agencies.

Footnote to 2.A.: SP 800-73 was posted April 8, 2005.

2.C.: The 3/15/2005 date for publication of the Implementation Management Handbook refers to a date in the past for a document that hasn't been finalized and is partially dependent of documents NIST hasn't finalized.

Section 3.Part 2.A-E. Just a note -- without the presence of a Government-wide PKI, full interoperability will be a huge challenge. More guidance on how to get to a Government-wide PKI is needed.

Section 3.Part 2.E. Recommend striking the entire last sentence. Priority of systems should be at the agency's discretion based on scope, and impact as defined in FIPS 199. Some agencies may prefer to not integrate high-impact systems first to gain implementation experience and maintain stability.

4.B.: Same comment as that for 2.C.

4.C: Recommend deletion of "in limited circumstances." The other caveats in the sentence are probably sufficient for security purposes, and we should encourage the widest possible Federal government scope for the card.

5.D. Add verbage which requires agencies to periodically re-review systems of records.

6.B.: Recommend reference to the National Security definition in FISMA rather than that in Clinger-Cohen. The drafters of the FISMA definition intentionally altered the scope from that contained in the Clinger-Cohen language.

7.C.: Change to - Implementation of Integrated Circuit Card Specifications - If your agency has not implemented a large scale deployment of identity credentials, you should implement the Part 2 specification stipulated in the standard and Part 3 of the accompanying Special Publication 800-73, Integrated Circuit Card for Personal Identity Verification. If your agency has a large scale deployment, you can use the interim transitional phase described in Part 2 of Special Publication 800-73.

Rationale: SP 800-73 has now been published. Finally, there is a question as to whether agencies may issues card with some of the functionality or look of PIV cards, but are not 100% PIV cards. For example, suppose an agency wants to issue cards to dependents but does

not want to do NACIs on them. Or, perhaps they want to issue cards to dependents that do not have PKI or biometrics. Since these folks are not employees/contractors, this would appear to be outside the scope of FIPS 201; however, such "PIV looking" cards could well cause confusion, since other agencies, etc. may believe they represent the same level of identity proofing as "full" PIV cards. This would appear to be a policy matter for OMB guidance.