Submitted by: _Tin T. Cao, Dept. of State - IRM/OPS/ITI/SI/IIB
Date: _1/19/2005

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
NIST SP 800-73						
1	State Department	Tin T. Cao	G	General to all sections	SP 800-73 is confusing. The verbiage talks to file system ("native") cards, but the technical specifications generally appear to favor a virtual machine ("Java") card, leaving agencies and card manufacturers guessing about the most appropriate type. Further, it appears to penalize those agencies who have already adopted a pure native or pure Java card. This is a conundrum that will force agencies into fielding PIV cards that do not fit their business case, operating environment, and/or security requirements; and, will force card/reader manufacturers into attempting to design and build a card that can be all things to all agencies, and consequently be excessively expensive.	Delay publication of SP 800-73 until FIPS 201 is published, technical requirements are clarified, and further inputs concerning Phase II implementation are known. Further, NITS should seek the participation and involvement of the GSC-IAB and its working groups (particularly the TWG and PAIIWG). **[Already Implemented in part per NITS decision o/a 11/18/2004]**
2	State Department	Tin T. Cao	G	General to all sections	SP 800-73 appears to ignore the previous work of the Interagency Advisory Board (IAB), and its subcommittees (TWG, PAIIWG, etc.). It mentions the standards developed by those activities, but then goes off in another direction--apparently pursuing a new ISO standard. Again, none of the agencies that had the foresight to adopt smart card technology have a card that will fully comply with this draft specification--necessitating all of those agencies to scrap their existing programs, lose the current investment, and spend additional funds to retool.	Put publication of SP 800-73 on hold at least until the final version of FIPS 201 is determined. In the mean time, turn over development of this SP to the GSC-IAB and its working groups (particularly the TWG and PAIIWG) for both technical review and coordination with industry to permit determination of what is and is not possible within given timeframes. **[Already implemented per NITS decision o/a 11/18/2004]**

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editorial, T = technical

Submitted by: _Tin T. Cao, Dept. of State - IRM/OPS/ITI/SI/IIB
Date: _1/19/2005

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
3	State Department	Tin T. Cao	G	General to all sections	It is doubtful that industry can produce a smart card that satisfies these specifications within the timeframe outlined in HSPD-12. As noted, the technical specifications are confused; neither building on previous efforts and standards nor posing a viable alternative standard for adoption. SP 800-73 is most pertinent to the Phase II implementation proposed in the revised FIPS 201.	Delay publication of SP 800-73 until technical requirements are clarified. NITS should advise OMB that the schedule outlined in HSPD-12 cannot be met because no smart card product, particularly one that combines the cryptographic and biometric technologies, will be available in that timeframe. **[Partially implemented per NITS decision o/a 11/18/2004]**
4	State Department	Tin T. Cao	G	General to all sections	SP 800-73 contains numerous spelling and grammatical errors. Before this document is submitted to the approving authorities, it should be reviewed by a technical writer. The primary problem lies in the "sense" of many portions of the text, not just in common spelling and grammar that is checked by a "spell check" function.	Conduct a full review of SP 800-73 by a technical writer/editor, in conjunction with a policy and/or technical expert.
5	State Department	Tin T. Cao	G/T	Section 1, pg 9 (fourth subparagraph)	This provision introduces confusion, in that it implies that either all cards must be capable of being read by any reader or that all readers must be capable of reading any card. While the desire to accommodate all possible solutions is understandable, it forces agencies to adopt an implementation methodology of all cards in all readers; making any / all existing systems non-compliant.	Recommend that one standard be adopted across the government, supported by an appropriate business case, and that those agencies with existing smart card systems be allowed to phase in the retrofitted new system over an extended period based on the anticipated life-cycle of their deployed systems.
6	State Department	Tin T. Cao	G/T	Section 1.1, pg 9	Again, this provision introduces confusion, in that it appears to allow either file system ("native") or VM card edges, but forces both to modify at least some portion of their operating system, card management, and/or middleware interface.	Recommend that one standard be adopted across the government, supported by an appropriate business case, and that those agencies with existing smart card systems be allowed to phase in the retrofitted new system over an extended period based on the anticipated life-cycle of their deployed systems.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editorial, T = technical

Submitted by: _Tin T. Cao, Dept. of State - IRM/OPS/ITI/SI/IIB
Date: _1/19/2005

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
7	State Department	Tin T. Cao	G/T	Section 5, pgs 26-50	Although SP 800-73 is (rightly) devoted to technical specifications, it highlights a major operational and security concern between "native" and VM cards--the controls over who controls administrative access to the card and how. The business case, and resulting security concerns, for some agencies necessitates that only specified offices can add, modify, and/or delete any type of data element stored to the card.	Recommend that some consideration be given to including at least minimal discussion of administrative card access in SP 800-73. The general policy for such controls should be included in FIPS 201, but this policy-procedural concern must cross-over between these two documents.
8	State Department	Tin T. Cao	G/T	Section 6, pgs 51-81	Again, there is no discussion of the administrative controls over implementation of these commands. Section 6, more so that Section 5, needs to address this critical issue and establish appropriate links back and forth between the technical and policy documents.	Recommend that some consideration be given to including at least minimal discussion of administrative card access in SP 800-73. The general policy for such controls should be included in FIPS 201, but this policy-procedural concern must cross-over between these two documents.
9	State Department	Tin T. Cao	G/T	Section 7, pg 82 (first & second subparagraphs)	These introductory comments to this section appear to be inconsistent and/or contradictory to the intent of the program, and with each other. The first subparagraph implies that interoperable use applications are mandatory--which is consistent with the apparent intent of SP 800-73, FIPS 201, and HSPD-12. However, the second subparagraph states that, "*Four card applications for interoperable use are described... All are optional card applications on a PIV integrated circuit card.*"	Clarify the intent of the PIV card, and modify the text of these two subparagraphs (and related text in Section 7) to reflect that either interoperability is the goal and that applications supporting interoperability are mandatory, or drop the goal of agency interoperability (at least for the time being) and make it very clear that implementation of any of these applications by any agency is optional to that agency.
10	State Department	Tin T. Cao	G/T	Sections 7.3.6 & 7.3.7, pgs 92-93	Related to the preceding comments regarding interoperability, the presence and functioning of the symmetric key for external/internal authentication must be clarified. If an agency chooses not to implement interoperable capabilities, then there does not appear to be a need for a symmetric key (at least for this purpose).	Again, clarify the intent of the PIV card relative to inter-agency interoperability.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editorial, T = technical