Submitted by: Will Liston
Willard.Liston@hhs.gov
Date: December 23, 2004

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
1	HHS/AHRQ	Bruce Immerman/Shelly Anderson	G- General &T-Technical	Section 5.2.1.1 - PIV Application and Approval - New Employees - page 42	The requirement that the results of the appropriate background check be received and adjudicated prior to the issuance of the PIV card will have a profound and deleterious effect upon the recruitment hiring process of prospective Federal employees, especially those who would fill non-sensitive positions. Currently, it takes an average of 4 months to receive a completed NACI report from OPM. If this requirement were to be implemented, prospective candidates for vacant positions would not opt for Federal employment. In the aggregate, the Federal Government would be severely hampered in discharging its responsibilities.	Temporary badges could and should be issued with limited access after the electronic fingerprint report has been favorably adjudicated. An appropriate unrestricted badge should be issued once the appropriate background check, i.e., NACI, was received and favorably adjudicated.
2	HHS/AHRQ	Bruce Immerman/Shelly Anderson	G- General & T-Technical	Section 5.2.1.2 - PIV Application and Approval - Current Employees - page 42	The application and approval process for current employees is problematic. For example, uniform standards have not been developed that define how often the NACI needs to be updated. In addition, OPM, through its contractors, would require a monumental infusion of resources to process requests to verify that NACIs have been conducted and/or to process routine background investigations. Moreover, OPM maintains its database for routine NACIs for 15 years. Therefore, it will be impossible to verify whether a NACI has been completed after 15 years.	A standard should be established for how long a NACI should be valid, i.e., 5 years, 10 years. Secondly, every Federal employee should be required to update their NACI even if it is a fingerprint check to provide updated information.
3	HHS/CDC/OCISO	Roger Johnson	T	Page 1, Section1, First Paragraph, Last sentence.		Need to add: (An accurate determination of identity is needed to make sound access control decisions) **and to generate an accurate audit trail.**
4	HHS/CDC/OCISO	Roger Johnson	G	Table 2-2, Row 1 (low)	Who does this level apply to? NACI (level 2 or higher) is required for Government employees. Isn't a NACI also required for contractors? Perhaps this is an interim clearance level while waiting for a higher level clearance?	

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

Submitted by: Will Liston
Willard.Liston@hhs.gov
Date: December 23, 2004

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
5	HHS/CDC/OC ISO	Roger Johnson	G	4.1.3.g	Are cards which are prepunched available, and can they be used? Prohibiting punching the PIV card with a hole to secure the card to a retractable lanyard will negatively impact usability. If not punched, it will have to be stored in a plastic see-through pocket (since it must be worn above the waist), which will make it difficult to use in contact readers (constantly putting in and removing from pouch). Perhaps it could be left up to the agency to determine if the card can be punched without damaging the circuitry?	
6	HHS/CDC/OC ISO	Roger Johnson	T	4.2, Paragraph 1, 2nd sentence	Section 6.1 of PACS (http://www.smart.gov/information/TIG_SCEPACS_v2.2.pdf) shows a Person Identifier field (which was apparently explicitly defined as Social Security Number in SEIWG-012). Because of the contactless interface which will exchange the FASC-N, it is very important that agencies not use SSN in the PI field, but rather some other agency unique person identifier (as strongly recommended by PACS). Also, authentication to third parties (i.e. application hosting providers running web sites, applications such as training, etc) will reveal the FASC-N to the third party. Prohibiting the use of SSN is very important for privacy and should be directly stated in FIPS 201—either as a recommendation or as a requirement. Due to the Privacy Act, the Government should not casually use SSN.	

Submitted by: Will Liston
Willard.Liston@hhs.gov
Date: December 23, 2004

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	HHS/CDC/OC ISO	Roger Johnson	G	Table 4-3, Row 2	Should "Position Sensitivity" be "clearance level"? For example, if someone is hired and completes the initial background check, but their full Background Investigation is not completed for a number of months, they will still need their ID and should be able to perform duties for which the initial background check is sufficient. So, even though their position is highly sensitive, the current clearance level of the person holding the card is only "low" or "1". When the clearance process is complete, their card could be updated to clearance level "4". If the person then transferred to a non-sensitive position, their clearance level is still "4" even if the position is level "1". If he/she unexpectedly needed to attend a sensitive meeting, his/her clearance level would be more helpful than the sensitivity level of his/her current official position.	
8	HHS/CDC/OC ISO	Roger Johnson	T	Section 4.3, 3rd paragraph, last sentence	This sentence states that "key pair generation" is a useful "optional" function. The bullets in the prior paragraph indicate that the function is required (as do the definitions in pages 28 and 29). Since interagency trust is required and each agency implements PIV independently, the surest way to have some certainty that private keys have not been inadvertently disclosed is for the keys to be generated on the card, with upload of only the public key to create the digital certificate. Otherwise, the validity of identity during authentication and of digital signatures is questionable. Keys should only be generated off-card when key escrow is required to ensure recovery of stored encrypted information (not applicable to authentication or digital signature keys).	
9	HHS/CDC/OC ISO	Roger Johnson	G	Table 5-1	References forms for Employment and Positions. Do all of these forms apply to contractors as well as federal employees?	

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

Submitted by: Will Liston
Willard.Liston@hhs.gov
Date: December 23, 2004

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
10	HHS/CDC/OCISO	Roger Johnson	E	5.2.3.2, 2nd Paragraph, 2nd sentence	States that cardholder must authenticate to the PIV card each time it performs a private key computation using the key management key. On page 29, the "Key Management Key" section provides conflicting guidance.	
11	HHS/CDC/OCISO	Roger Johnson	T	B.2, 1st Paragraph, 1st sentence	Incorporates 800-63, but that SP is only applicable to externally facing systems ("The recommendation (SP 800-63) covers remote authentication of users over open networks."). FIPS 201 is for "internal" users (employees and contractors)— for their access to internal and external systems. The qualification in SP 800-63 causes a conflict. Is B-2 only applicable to externally facing systems?	
12	HHS/CDC/OCISO	Roger Johnson	T	Table B.2	This table indicates (implicitly) that the PIV card is only mandatory for Assurance Level 4. HSPD-12 seems to require more widespread use. Can you explicitly state when the PIV card must be used, versus when it is optional, or will OMB clarify?	
13	HHS/CDC/OCISO	Roger Johnson	E	Table 4-3, Row 1 (Expiration Date)		Typo? Should the expiration date format be yyyymm**dd**? Or is it understood that the card will expire on the last day of the given month?
14	HHS/CDC/OCISO	Roger Johnson	E	4.4.5.5, 2nd Paragraph, 2nd sentence		Typo. Replace *image* with *images*
15	HHS/CDC/OCISO	Roger Johnson	E	4.4.5.6, 1st Paragraph, 1st sentence		Typo. Replace *system* with *systems*

Submitted by: Will Liston
Willard.Liston@hhs.gov
Date: December 23, 2004

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
16	HHS/CDC/OCISO	Roger Johnson	T	Table 2-2, page 6 Table B-2, page 65	FIPS 199 is THE standard for categorizing the sensitivity of federal information systems, having been established as the first step in information security (categorize the system, then use the results to determine which controls are required, then assess to determine if the controls have been implemented properly). It is not clear that the position sensitivity levels defined in Table 2-2 directly correspond to the same-named levels in FIPS 199. Direct coorelation would mean, for instance, that a FIPS 199 MODERATE system requires a minimum NACI background check for all system users, and all users of a FIPS 199 HIGH system would require at least a NACIC (individual systems always have the option to select a higher control than the minimum). Table B-2 does not show which assurance level is the minimum required for each FIPS 199 categorization, though OMB M-04-04 hints at the coorelation (Assurance Level 2 = FIPS 199 category LOW, 3=MODERATE, and 4=HIGH) based on confidentiality.	As in FIPS 200 (SP 800-63), tie all controls (such as personnel background checks and authentication assurance levels) back to FIPS 199, so it is clear which control is the minimum for each FIPS 199 categorization.

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

Submitted by: Will Liston
Willard.Liston@hhs.gov
Date: December 23, 2004

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
17	HHS/NIH	Mark Silverman	Technical	4.2, Page 25	**Due to a technical problem which we were unable to resolve (even by completely rekeying the text). We were unable to get the text to wrap properly throughout this cell and be readable. Therefore a Word document is attached with the entirety of comment line 17 for HHS/NIH. It is named - HHS-NIH Comment on Draft FIPS 201 Standard (HSPD-12).** The PIV card must have a Persistent Federal Identification Number (PFID) associated with each card holder. A PFID is necessary to support the PIV-1 identity proofing and registration process (Section 2.2, Page 4) and enable the use of the PIV card's digital certificate to provide logical access to Federal IT systems. A PFID is needed to cross-reference and link the various stages of the identity proofing process together. The PFID will enable reference to historical data, such as the subject's previous criminal background checks (Section 2.2.2, Page 7). Without the PFID, it will be very difficult to correlate an individual's PIV actions across multiple Agencies and/or employment relationships (e.g., contractor becoming a Federal employe	A possible approach for implementing a persistent Federal identification number (PFID), within the construct of the current FIPS 201 standard, would be to have the "optional" 16 character GUID field of the CHUID (PACS 2.2 Guidance, page 10), become the "required" PFID. The format of this number could be similar to the FASC-N, in that the first 8 characters be the Agency and System code of the original issuer. Once issued, the first 8 characters would have no special meaning other than to ensure uniqueness. Alternatively, the 10 character PI field of the FASC-N could serve as the PFID, except that the longer GUID field provides a better mechanism (as suggested) to ensure uniqueness. The GUID field could replace the FASC-N in the certificate's subject alternative name extension or be added to the subject's distinguished name (DN) as a UID attribute (OID 0.9.2342.19200300.100.1.1). This later approach would help ensure name uniqueness within the DN and also provide out-of-the-box interoperability with commercial authentication solutions (e.g., Netegrity's Siteminder).
18	HHS/PSC	Tim Brown	G	Numerous pages		As of October, 2005, begin phasing-in of new program by using the PIV requirements for all new employees and contractors. Begin phasing-in of new PIV requirements for current employees and contractors as their current badges expire, up to a three to five year period.

Submitted by: Will Liston
Willard.Liston@hhs.gov
Date: December 23, 2004

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
19	HHS/PSC	Tim Brown	G	Numerous pages	Waiting for the highest level background check for an individual prior to badge issuance could take several months.	Perform minimum check before badge issuance, then add higher level security to the card once the higher level security is approved. Entry to higher level facilities or information would require an escort/monitoring until the higher level of security clearance is approved.
20	HHS/PSC	Tim Brown	T	4.1.3.g. - page 18	Clause requires that the ID not have a hole punched in them; for use in access systems that require contact readers (Weigand, magstripe, bar code), the ID must be readily accessible without having to remove it from a pouch. The easiest method to have the ID access these style readers is to have the card available by using a hole punch and have the card exposed on a lanyard or some other holding/display device.	Allow hole punches on the top of the ID for the display device (lanyard, reel, clip, etc.).

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