Submitted by: ______________________

Date: __________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
1	NSA, R223	Lawrence Reinert	G	All	There is not enough discussion on the maintenance and usage of the PIV (PIV authentication, Local authentication, digital signature, key management, and card and card management keys) to make a determination on the interoperability, security, maintenance requirements, or application of the keys.
2	NSA, R223	Lawrence Reinert	G	All	Although the PIV spec addresses the use of AES and ECDSA, it does not discuss the transition of the PIV of the algorithms. It does not address the support for MQV of other key agreement mechanism. The document does not discuss the impact to the PKI for such a transition.
3	NSA, R223	Lawrence Reinert	G	All	The specification addresses PIV User Authentication in terms of a PIN or biometric. PIV user authentication should be clearly defined as a set of mechanisms in which PINs or Biometrics can be part of (to allow future mechanisms). A process should be defined in which an agency can submit for PIV approval of a new mechanism.
4	NSA, R223	Lawrence Reinert	G	All	There is no discussion on the issuance of a temporary PIV (or equivalent) if the PIV is misplaced, or forgotten.
5	NSA, R223	Lawrence Reinert	G	All	There is not enough detail on the use of signature on the biometric data and the CHUID to determine if proper assurance is given to the handling and verification of the data.

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

Comment template for draft FIPS 201 and SP 800-73

Submitted by: ______________________________

Date: __________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
6	NSA, R223	Lawrence Reinert	G	All	The SCEPACS referenced for the contactless interface does not provide enough information to make an determine on the security of the high assurance profile. For example it reference a TBD algorithm to be used to create a secure session and does not seem to require channel encryption for the transfer of data between the card and the reader. Use of the low (and possibly medium) assurance profile should be discouraged.
7	NSA, R223	Lawrence Reinert	G	All	There should be some attempt to create government wide PIV standard applications. This can reduce the cost of these applications, increase user familiarity, and reduce the need for duplicative efforts between agencies.
8	NSA, R223	Lawrence Reinert	G	All	PIV maintenance is not thoroughly discussed.
9	NSA, R223	Lawrence Reinert	G	All	The use of biometrics does not fit the current storage or I/O capability of smartcards. Specifically the defining images and not templates leads to much larger data storage items than can be properly handled by a typical smart card application.
10	NSA, R223	Lawrence Reinert	G	All	The document refers to terms that are defined by ISO 7816 that imply the use of file system cards and should be rephrased to imply the use of either File system or virtual machine (i.e. java) cards.
11	NSA, R223	Lawrence Reinert	G	2.2.1	Position Sensitivity Level is not properly discussed. The glossary infers the term is defined by the OPM, but no reference to the exact OPM source is given.

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

Submitted by: ______________________________________

Date: ______________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
12	NSA, R223	Lawrence Reinert	T	2.2.1	What assurances does the PIV Authorizing official have that the document received from the PIV Requesting Official have not been altered? It seems like this process could be automated and make use of digital signatures to provide integrity services.
13	NSA, R223	Lawrence Reinert	T	2.2.3	This section implies that short term credentials can be issued. A larger discussion on short term credentials is needed.
14	NSA, R223	Lawrence Reinert	E	2.2	A Flow chart or diagram would help this section.
15	NSA, R223	Lawrence Reinert	T		It would seem an applicant would have to show up in person three separate times to be issued a PIV. This process could be streamlined.
16	NSA, R223	Lawrence Reinert	T	3.2.1	NIST should explore making the registration information standard so they can be used by other agencies or for future employment. Having this information standardized in an electronic format with validating electronic signature would be a very powerful piece of information.
17	NSA, R223	Lawrence Reinert	T	3.3.1 and 4.1.6	The use of a PIN pad versus alphanumeric input severely restricts the number of possibilities for knowledge based verification and is difficult for users to remember.
18	NSA, R223	Lawrence Reinert	T	3.3.1 and 4.1.6	There should be alternatives to using the PIN to unlock the card (such as a challenge response protocol). Using a PIN should be optional.
19	NSA, R223	Lawrence Reinert	T	4.1.2.a	Use of optical components or layers on the card substrate provide little or no benefit for tampering. The reliance of visual inspection adds little benefit to the card validation process since there is a trend for automating the authentication process.

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

Submitted by: ____

Date: _______________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
20	NSA, R223	Lawrence Reinert	T	4.1.2.b	There should be a method of querying the PIV to determine which anti-tamper mechanisms have been implemented. This will allow the authentication process to help determine the assurance of the device.
21	NSA, R223	Lawrence Reinert	T	4.1.3.a	Please state which contact and contactless interfaces are required.
22	NSA, R223	Lawrence Reinert	T	4.1.6.1	The sending of authentication data to the card should require a trusted path (e.g. an encrypted channel) to insure the protection of the data sent to the card. PINs can be hashed on the host side to insure that pin values entered at the PIN PAD are not read through the PIV interface.
23	NSA, R223	Lawrence Reinert	T	4.1.6.1	The use of a challenge/response to unlock the card should be optional. This will allow for alternate off card verification of the user.
24	NSA, R223	Lawrence Reinert	T	4.1.6.1	Biometric Match on card technology should meet the FIPS 140-2 requirement for random attempts at the authentication just like the PIN. This equates to a FAR. This document should address the FAR requirement for Match on Card biometric technology. In the past, MOC technology has proven to fall far short of meeting this requirement. NIST may be allowing very weak authentication to occur on the card.
25	NSA, R223	Lawrence Reinert	T	4.1.6.1	Standardization of the Match on Card technique should be addressed in the specification.
26	NSA, R223	Lawrence Reinert	T	4.1.6.1	PINS should be stored on the card as a hash or encrypted value. Protection of biometric information on the card should also be discussed

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
27	NSA, R223	Lawrence Reinert	T	4.1.6.2	The GP discussion should include separate GP security Domains so as to support delegated management. Separate security domains will be needed to support the higher assurance applications.
28	NSA, R223	Lawrence Reinert	T	4.1.6.2	GP card managers should be required to handle asymmetric keys for their secure channel.
29	NSA, R223	Lawrence Reinert	T	4.3	The PIV should NOT restrict the use of cryptography over the contactless interface. That is where it is needed the most!
30	NSA, R223	Lawrence Reinert	T	4.3	The PIV should not discourage the implementation of hashing on the PIV. Many smart cards and other tokens are now capable of handling many hashing functions in a reasonable amount of time.
31	NSA, R223	Lawrence Reinert	T	4.3	This standard should address interoperability requirements for contactless interfaces. Interoperability includes the use of cryptographic handshakes, key management, and data exchanges used for basic authentication.
32	NSA, R223	Lawrence Reinert	T	4.3	Table 4-3 should include ECC as the PIV may be required to use an encrypted channel for certain key or card management functions.
33	NSA, R223	Lawrence Reinert	T	4.4	Details are needed on the fingerprint capture, quality requirements, system storage, translation, etc.
34	NSA, R223	Lawrence Reinert	T	4.4	ANSI INCTIS 381 specifies an Image based format. Image format may take up to 100K bytes per image. ANSI INCITS 378 (minutia based) templates should be used. These will be on the order of less than 500 bytes per print.

Submitted by: ______________________________

Date: ______________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
35	NSA, R223	Lawrence Reinert	T	4.4.5.5	The data size indicated in this section is extremely large for a ISO 7816 card. Suggest making option to reduce the data size. AS an example a small grayscale image can be used for human verification situation where the high resolution may not be required. Most smart cards can't store this much information (e.g. <64K). The time to extract this from the card would be too long as well.
36	NSA, R223	Lawrence Reinert	T	4.4.2	Complying with ISO 14443 does not imply any interoperability. This specification should seriously consider looking into contactless interoperability. It will save the government millions of dollars in the long run.
37	NSA, R223	Lawrence Reinert	T	4.4.2	The use of PCSC over the contactless interface has yet to be tested on a significant number of cards. Many contactless chips will not be able to provide useful functions over this interface. FIPS 201 should look closer at contactless requirements.
38	NSA, R223	Lawrence Reinert	T	4.5.3	Incorporating the keypad into the reader or keypad increases the cost of the reader or keyboard. It only provides a benefit if the reader provides the data directly to the PIV without going through the Host system. This implementation will not allow a trusted path to the PIV since readers are not likely to be installed with a keyset and the necessary processing capability.
39	NSA, R223	Lawrence Reinert	T	5.2.1	This section is a duplication of section 2.1.1
40	NSA, R223	Lawrence Reinert	T	5.3.2.3	The X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework does not have support for ECC and ECDSA as required (optionally) by this specification.

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

Submitted by: ______________________________________

Date: ______________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
41	NSA, R223	Lawrence Reinert	T	5.4.2.4	Minimum requirements for resetting a PIN should be discussed in this document. Lax requirements for PIN resetting can lead to an easy path for using lost or stolen cards that are not reported.
42	NSA, R223	Lawrence Reinert	T	6.1.4	The use of symmetric key based challenge response schemes should be avoided. The Card has several asymmetric keys and should be able to support a challenge response mechanism based on an asymmetric key set on the contact interface. Symmetric key authentication should be limited to the contactless interface when asymmetric keysets are not available.
43	NSA, R223	Lawrence Reinert	T	6.1.4	The Symmetric Authentication should be detailed in SP800-73 or the corresponding contactless description.
44	NSA, R223	Lawrence Reinert	T	6.1.5	A preference of using asymmetric authentication should be made to encourage its use over the symmetric version.
45	NSA, R223	Lawrence Reinert	T	6.1.5	The protocol and APDUs used to implement the authentication scheme should be detailed in SP800-73.
46	NSA, R223	Lawrence Reinert	T	6.2	The Physical access Control protocol should be one of the previous specified protocols.
47	NSA, R223	scluthe	T	4.2.2	Table 4-4 should include SHA-384 & SHA-512 to support National Security Systems
48	NSA, R223	scluthe	T	4.2.2	Table 4-5 should specify ECC MQV as defined in NIST Special Pub 800-56
49	NSA, R223	scluthe	T	6.1	Remove " For privacy reasons, contactless use of PINs and biometrics is not supported."

Submitted by: ______________________________

Date: ______________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
50	NSA, R223	scluthe	T	6.1.2	"container that is an Elementary File (EF)." restricts the use of java cards.
51	NSA, R223	scluthe	T	6.1.2	Low profile is exceptionally weak.
52	NSA, R223	scluthe	T	6.1.5	The steps of the authentication do not maximize protection to the user's authentication information.
53	NSA, R223	scluthe	T	6.2	The PACS Authentication for Physical Access Control seems unnecessarily weak compared to that for logical access.
54	NSA, R223	scluthe	T	6.3.2	logical access limited to RSA exchange

Proposed change
A completed card management specification should be developed to address these concerns.
Add further discussion on the transition to newer algorithms including key management issues. Add a discussion on ECC based key agreement.
Add a discussion on user authentication mechanisms. Add a process for creating new mechanisms including other biometrics, card authentication protocols, and passwords and pass phrases.
Add a discussion on temporary PIVs.
Add a section on the verification of non key related information placed on the PIV. Include the relation to the PKI and how revocation of the data issuer is to be handled.

Proposed change
Add missing details to the SCEPACS pacs document in an appendix or make necessary updates to SCEPACS.
Add a discussion on common applications. This could include PIV maintenance application.
Add a discussion on maintenance concepts for user portals or other techniques for managing PIV data.
Use the NCITS defined fingerprint template and reduce the picture image size to a smaller image for use on the smart card.
Change Root directory to globally acceptable object. Change Elementary and transparent file objects with the appropriate access control.
Place a reference to the source the Position sensitivity level in the glossary and in the reference documents.

Comment template for draft FIPS 201 and SP 800-73

Submitted by: ______________________________

Date: ______________

Proposed change
Add requirements for the PIV authorizing official to validate documents using digital signatures.
Add a discussion on short term credentials.
Add a flow chart.
Require anti-tampering methods that can be detected by the PIV and prevent its operation if the tamper is detected.

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

Submitted by: ______________________________

Date: ____________

Proposed change
Require the a means of being able o detect a tamper and respond to the access control subsystem with an indication of tampering.
Add a requirement to encrypt or has data sent authentication data sent to the card.
Add a statement to insure that Match on card technology be required to meet the requirements in FIPS 140-2 section 4.3.3
Add a section on Match on Card technical details
Add a section discussing the on card protection of authentication data.

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

Submitted by: ____

Date: _______________

Proposed change
Add RSA 1024, RSA 2048, and ECC 384
remove the sentence forbidding the use of cryptography over the contactless interface.
Add a discussion on the benefits of hashing on the PIV.
Add a section to discuss Contactless Requirements.
Update the Table to include ECC 160 or higher.
Add a lot more details to the fingerprint processing section.
Suggest using ANSI INCITS 378. This will reduce the storage (and I/O requirement) for the use of the Biometric on the PIV.

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

Proposed change
Add a section with an option for storing the facial image. Store the facial images in separate files to allow the selection of different images.
Add a section defining interoperability requirements for contactless cards.
Add a note on the use of PCSC with contactless cards.
Add a statement to require the PIN to go directly to the PIV from the reader.
Refer to section 2.2.1 and reduce the size of this section.

Submitted by: ____

Date: _______________

Proposed change
Add a section discussing the PIN reset requirements. A fingerprint verification (at a minimum) should be required.
Restrict the use of symmetric authentication to the contactless interface.
Add SHA-384 & SHA-512
Add ECC MQV 384 bit keys under Key Management Key to support National Security Systems.
Contactless use of PINs and biometrics does not compromise user's privacy with the proper use of encryption.

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

Proposed change
Reword to describe it's storage as a EF or java card applet.
Ban the use of the low profile. Require use of optional steps 2 & 3 of medium profile.
The sequence should be altered so that the card & infrastructure mutually authenticate and provide a cryptographically secure link between the keypad & the token so that the user's authentication data is not exposed.
Every effort should be made to improve physical security authentication to equal that of logical access.
Expand to reflect available asymmetric cryptography options (RSA, ECDSA, ECC-MQV)