Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
3M-1	3M	Ella Schiralli	E	page 28 -32 the draft	photo images	Figures 4-1 through 4-5	Section 4.1.4.1 Mandatory Items on the front of the PIV Card [page 23, line 940] references the photograph with no requirement that the photograph be color. Black and White photographs should be acceptable as many of the highest value ID credentials [i.e.USA ePassport cards, Driver's Licenses] are moving to more secure laser engraved ID card construction that use Black and White photographs. This technology is helpful in increasing physical ID card security and mitigating impersonation fraud. Photographs should be either color or black and white and subject to existing photograph quality standards.	Remove the word COLOR from the figures on line in line out draft version pages 28-32 to simply read PHOTOGRAPH.	Declined. Studies have shown that humans can perform facial comparisons more accurately with color photographs than with black and white photographs. Furthermore, in order to maintain commonality among PIV Cards issued by different agencies it is important to limit the degree of variability that is permitted.
3M-2	3M	Ella Schiralli	G	page 6 in the draft	384	2.3 first bullet	The proliferation of high quality counterfeit documents coupled with the increasing integration of ID document security features places an unrealistic burden on individuals to spot a fake or compromised ID document during the review of idenity source documents in enrollment. Agencies should be required to utilize document authentication solutions to analyze identity source documents for added machine readable verification of the document's authenticity. Document authentication analysis is an excellent added tool for ID Proofing the identity being claimed. The first step in building a “Chain of Trust” for the PIV is authentication of the primary source documents.	at the end of line 1, bullet 1 in section 2.3 add the 'bold' words […and registration process **'which includes the use of document authentication and verification solutions'** in association with…]	Declined. The first bullet of Section 2.7 states that "The organization shall adopt and use an approved identity proofing and registration process in accordance with [SP 800-79]." This is not an appropriate place to specify requirements for the identity proofing and registration process. See also AT-2.
3M-3	3M	Ella Schiralli	G	n/a	n/a	n/a	3M has performed a forensice analysis on counterfeit documents and is providing it as an attachment for your background and consideration: "3M Counterfeit Driver's Licenses"	Attachment supporting recommendation above.	Noted.
AMAG-1	AMAG Technology	Adam Shane	T	2	260	1.3.1	It is not clear how any change to the standard can be considered backward compatible. A change that would be backward compatible to a relying system, would not be backward compatible to a PIV Issuance system, and vice versa. For example, if an optional element is made mandatory on the card, this is not backward compatible to the PIV issuance system that did not implement the optional field.	There are no changes to the standard that can be considered backward compatible across the board.	Declined. See AMAG-1 in disposition of comments for the March 2011 Draft FIPS 201-2.
AMAG-2	AMAG Technology	Adam Shane	G	3	282	1.3.4	While it is understood that re-use of deprecated features seems like good change management, this is a significant challenge for relying party systems. Deprecated features are not backward compatible, and this section even indicates that such features remain in the standard.	If deprecated features remain optional in the standard, there is no reason to remove them on replacement of the card. Remove statement from standard.	Declined. Since deprecated features will be removed from the next version of FIPS 201, this statement suggests that new product should not implement deprecated features.
AMAG-3	AMAG Technology	Adam Shane	T	3	287	1.3.5	Other components that may be affected by version management include components or systems that rely on PIV cards or their data.	Add to the last sentence of the paragraph, "and components or systems that rely on PIV cards or their data."	Declined. The list provided is an example only and it is not meant to be exhaustive
AMAG-4	AMAG Technology	Adam Shane	T	3	291	1.3.5	Identification of optional features through an on-card discovery mechanism may be extremely time consuming and is not appropriate for PACS solutions.	The last sentence of the paragraph should be enhanced to indicate that on-card discovery mechanisms may have a detrimental impact on the time needed to read and interoperate with the card by relying systems.	Declined. Discovery mechanism(s) is necessary to be on the card but there is no requirement for relying systems to use the discovery mechanism.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AMAG-5	AMAG Technology	Adam Shane	T	6	402	2.4	Fingerprint templates for on-card comparison may be the same as the fingerprint templates that are released from the card for off-card comparison. This should be forbidden - if an attacker manages to obtain the templates, they can be used to generate a simulated fingerprint image and provided to the card for OCC operation to activate the card. Section 4.2.3.3 specifically states, "The fingerprint templates for on-card comparison shall not be exportable." If these are the same templates as used for off-card comparison, they cannot be exported even if stored in different locations on the card.	Modify requirement on line 402 to read, "Two fingerprints, for on-card comparison, which shall be from different fingers than the fingerprints collected for off-card comparison."	Resolved by changing the sentence to read: Two fingerprints, for on-card comparison. It is recommended that these be different than the fingerprints collected for off-card comparison. Note: SP 800-76-2 includes a note about the usability versus security tradeoff associated with cardholder confusion concerning which finger to present.
AMAG-6	AMAG Technology	Adam Shane	T	7	429	2.5	The standard allows for use of electronic facial image for authentication in operator-attended PIV issuance, but does not consider use of this authentication mechanism for use in PACS.	Statement at line 429 should be expanded to add, "or other operator-attended authentication operations."	Declined. Comparison of electronic facial images can only be performed reliably in environments that are carefully controlled for such issues as lighting, and so it is not appropriate for use as a general-purpose authentication mechanism, even in operator-attended environments.
AMAG-7	AMAG Technology	Adam Shane	E	12	606	2.9	"PIV card update" is referred to as PIV card renewal in following section 2.9.1.	Section 2.9 should be updated for consistency.	Resolved by merging sections on renewal and reissuance. "PIV Card update" refers to performing post-issuance updates of the data on the card.
AMAG-8	AMAG Technology	Adam Shane	T	13	628	2.9.1	If the original PIV card is lost, stolen between time renewal is requested and time card is issued, then the card cannot be surrendered. However, it would inefficient and expensive to abandon the renewal process and start a re-issuance process at that time (HSPD-12 refers to government effeciency).	In line 628 "shall" is to be replaced by "should", and the statement to be augmented with direction to revoke certificates and other appropriate operations if the card is not available for surrender.	Resolved by AMAG-11.
AMAG-9	AMAG Technology	Adam Shane	T	13	635	2.9.1	The standard states that biometric authentication accuracy degrades with time elapsed since initial collection. I don't believe this is a generally held belief. If NIST has empirical studies to back up this statement they should be referenced in a footnote.	Remove the offending statement. It becomes a policy decision, not based on scientific data but on a desire to limit risk.	Declined. See comments such as Cert-30, Cert-37, and DoD-52 in the disposition of comments for March 2011 Draft FIPS 201-2. Commenters felt that it was very important to note that issuers had the option to recollect biometric data more frequently than required by the standard. As noted, the decision to collect data more frequently than required is an agency policy decision.
AMAG-10	AMAG Technology	Adam Shane	T	13	639	2.9.1	If the PIV Authentication Key is designated as a person authentication, then it should not be re-issued when a new PIV card is created. The CAK, on the other hand is a card authentication key and should be re-issued. Furthermore, if certificates are re-issued, then the older certificates should be revoked.	Section 2.9.1 should be updated to include the revocation of the old keys if new keys are issued.	Declined. Section 4.2.2 states that the PIV Authentication key shall be generated on the card and that the PIV Card shall not permit exportation of the private key. Since the private key cannot be moved from one card to another, a new PIV Authentication key must be generated on the new card and a new, corresponding PIV Authentication certificate must be issued. See GSA-18 in disposition of comments for March 2011 Draft FIPS 201-2 for reason that revocation of older certificates is not mandated.
AMAG-11	AMAG Technology	Adam Shane	G	14	687	2.9.2	Procedures for renewal and re-issuance are very similar and should be combined. This also fits with recommendation in AMAG-7 above.	Procedures for renewal and re-issuance are very similar and should be combined. This also fits with recommendation in AMAG-7 above.	Accept.
AMAG-12	AMAG Technology	Adam Shane	T	14	689	2.9.3	Part of Agency policy should be to notify the individual when data on their PIV card changes. They should be notified of what changed, and why.	The standard should be updated to require Agencies to modify their privacy policy to notify individuals when their PIV card data is modified, and when backend systems data about them is modified.	Declined. As noted, this would be a matter for an agency's privacy policy and covered by the SORN.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AMAG-13	AMAG Technology	Adam Shane	G	15	708	2.9.4	IT best practices indicate PIN reset should be done every 90 days. In case of existing PIN being known, OCC not required - 2.9.4 assumes PIN is forgotten, but perhaps generically Card Data Reset should require three-factor authentication.	NIST to consider how to bring PIV card into compliance with 90-day PIN reset recommendations. 2.9.4 should require three-factor authentication.	Declined. While it is common practice to require passwords to be changed on a regular basis (e.g., every 90 days), this does not apply to PINs that are used to authenticate to a smart card. Declined. The purpose of the reset operation is to address the case in which one of the factors is not working (e.g., the cardholder has forgotten the "something you know" factor). Requiring three-factor authentication would defeat the purpose of reset.
AMAG-14	AMAG Technology	Adam Shane	T	16	749	2.9.5	A negative background investigation report received after the issuance of the card should be cause for card termination. Also, if agency uses Continuous Information Management Engine (CIME) and it returns negative information, this may also be cause for card termination.	Update 2.9.5 to include additional reasons that may be cause for PIV Card Termination.	The second bullet in Section 2.8 in Revised Draft FIPS 201-2 says "The PIV Card shall be revoked if the results of the background investigation so justify." Accept to change "revoked" to "terminated" and to add this as a reason for termination to Section 2.9.5 (now Section 2.9.4).
AMAG-15	AMAG Technology	Adam Shane	E	16	759	2.9.5	It is not clear what it means to "revoke" a PIV card. Does this mean the certificates are revoked? Or should this term be changed to "terminated" as is used on lines 775 and 776?	This statement should be modified or clarified.	Resolved by specifying in Sections 2.9.1 and 2.9.5 (now Section 2.9.4) that a PIV Card is revoked by performing the steps: + The PIV Card shall be collected and destroyed, if possible. + Any databases maintained by the PIV Card issuer that contain FASC-N or UUID values from the PIV Card must be updated to reflect the change in status. + If the PIV Card cannot be collected and destroyed, the CA shall be informed and the certificates corresponding to the PIV Authentication key and asymmetric Card Authentication key shall be revoked. If present, the certificates corresponding to the digital signature key and the key management key shall also be revoked.
AMAG-16	AMAG Technology	Adam Shane	E	17	788	2.11	HSPD-12 does not say that the control objectives are the only applicable uses of the PIV card.	NIST should not be changing the meaning of HSPD-12. The statement should be removed or modified to state, "No department or agency shall implement a use of the identity credential that is in contradiction to any of these control objectives."	Declined. The statement as written does not preclude uses of the PIV Card for purposes other than those specified in the control objectives, as long as those uses are not "inconsistent" with the control objectives.
AMAG-17	AMAG Technology	Adam Shane	T	18	818	2.11	Employees should not be making the decision to protect their PIV data through an electromagnetically opaque holder. This should be a CPO decision that flows into Agency policy.	Modify the statement to read, "Specifically, Agencies may choose to deploy PIV credentials with electromagnetically opaque holders…"	Resolved by revising the sentence on line 818 to: "Agencies may choose to deploy PIV Cards with electromagnetically opaque holders or other technology to protect against any unauthorized contactless access to information stored on a PIV Card."
AMAG-18	AMAG Technology	Adam Shane	E	20	861	3.1.1	Card readers are also located at registration and issuance stations.	Update the statement.	Declined. This is what the card writers are used for in the 3rd paragraph.
AMAG-19	AMAG Technology	Adam Shane	T	42	1293	4.2.2	Secure messaging should be a requirement of the card issuance so that relying parties can optionally use this mechanism to establish a virtual contact interface.	Standard should read, "The PIV Card *shall* include an asymmetric private key…"	Resolved by SIA-7.
AMAG-20	AMAG Technology	Adam Shane	T	43	1352	4.2.2	Missing statement regarding appropriatness of the virtual contact interface.	Add support for the virtual contact interface.	Declined. See Cert-80 in disposition of comments for March 2011 Draft FIPS 201-2.
AMAG-21	AMAG Technology	Adam Shane	T	45	1425	4.2.3.3	On-Card Comparison (OCC) is also a valid means of activating the card for biometric data access unless AMAG-26 is accepted.	Add support for OCC to activate the card.	Declined. Biometric data may only be read from the card if the card has been activation using PIN-based authentication. OCC may be used to activate the PIV Card to perform private key operations, but not to read the biometric data from the card.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AMAG-22	AMAG Technology	Adam Shane	T	46	1441	4.2.4	The standard does not include a mandatory UUID for explicit cardholder identification. If working in an offline scenario (First Responders at a disaster site, for instance) one cannot rely on an association with unknown credential identifier and the issuer's person identifier. Therefore, the person identifier should be on the card. While this is true for FASC-N, it is not true for PIV-I and in order to be consistent in this regard between PIV and PIV-I (for efficiency's sake) should be mandatory in PIV.	The standard should require a UUID based Person Identifier.	Decline to make a UUID based person identifier mandatory. However, the initial draft of SP 800-73-4 includes a Cardholder UUID as a data element that may optionally be included in the CHUID.
AMAG-23	AMAG Technology	Adam Shane	E	50	1561	5.5	Similar to AMAG-15, the phrase, "card is revoked" is used here and should remain consistent with other terminology.	The statement should be modified or clarified.	Resolved by AMAG-15 and by changing the sentence in Section 5.5 to read: If the card is revoked, the authentication certificates shall be revoked in cases where the card cannot be collected and destroyed.
AMAG-24	AMAG Technology	Adam Shane	T	52	1594	6	The section only outlines authentication mechanisms that utilize the PIV Card, but the standard is often interpreted to represent system-level requirements. Therefore, some recognition should be included of authentication mechanisms that are outside the scope of the PIV card.	Add statement to the effect, "Other authentication mechanisms that do not rely on data stored in (logical) or on (physical) the PIV card should be approved by the Agency as having similar levels of confidence as those present on the PIV card." Alternately, the statement could be, "Other authentication mechanisms that do not rely on data stored in (logical) or on (physical) the PIV card may be used but are outside the scope of this standard."	Declined. The purpose of Section 6 is to describe authentication mechanisms that can be implemented using the PIV Card. Reference to authentication mechanisms that do not make use of the PIV Card would be confusing, especially in light of mandates such as OMB M-11-11, which states that "each agency should develop and issue implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems."
AMAG-25	AMAG Technology	Adam Shane	T	53	1645	6.2	Card readers are not limited to the contact or contactless variety. Card readers may or may not have biometric capture or PIN entry capabilities.	Sentence should read, "Card readers, when present, can be contact readers or contactless readers; and they may or may not have biometric capture and PIN entry capabilites."	Declined. Even card readers that have integrated biometric capture or PIN entry capabilities are either contact or contactless (or both), so the statement is not inaccurate, and there is no need to mention in this section that card readers may have integrated biometric capture or PIN entry capabilities.
AMAG-26	AMAG Technology	Adam Shane	T	55	1684	6.2.2	On-Card Biometric Comparison (OCC-AUTH) is inappropriate for PIV card use. The premise of authentication mechanisms in PIV program are to use trusted information. OCC assumes the fingerprint image submitted to the card is a valid capture of a live fingerprint scan. The data cannot be trusted unless the card trusts the reader, and there is no mechanism for this.	OCC must be removed from consideration in the PIV program until various technical details can be worked out.	Declined. OCC has been requested by many agencies. Section 6.2.2 only discusses authentication and in this case the relying system is in control of the reader for authentication.
AMAG-27	AMAG Technology	Adam Shane	T	55	1709	6.2.3.1	It is interesting that the user submits a PIN to the card before the card is authenticated. If the card were a counterfeit, it could be collecting the PIN information from the user to be used in a later attack.	Best practices indicate to authenticate the card prior to providing any private information to the card (PIN or biometric data). PKI-AUTH and OCC violate best practices and should be reconsidered.	Declined. While a counterfeit card could collect any PIN data or biometric samples provided to it, the user who is being attacked would have to provide both the counterfeit card and the PIN or biometric sample to the reader, so the attacker would have to trick the cardholder into using the counterfeit card in order for this attack to work, and would then need to obtain both the counterfeit card and the actual PIV Card in order to be able to make use of the data collected by the counterfeit card. While it would be technically possible to authenticate the card using the PKI-CAK or SYM-CAK authentication mechanism before submitting the PIN or biometric sample to the card, this would be very inefficient, and for the reasons described above, unnecessary.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AMAG-28	AMAG Technology	Adam Shane	E	59	1819	6.3	Section 6.3 seems to have been moved in relation to the authentication mechanisms of section 6.2. Now the statement, "The following subsections specify…" is no longer valid - what follows is not a specification as in 6.2.	Change the statement to read, "The following subsections *categorize* the …"	Resolved by changing: The following subsections specify the basic PIV authentication mechanisms that may be used to support the various levels of identity authentication assurance as defined in Section 6.1. To: The following subsections specify which basic PIV authentication mechanisms may be used to support the various levels of identity authentication assurance as defined in Section 6.1
AMAG-29	AMAG Technology	Adam Shane	E	59	1825	6.3	In addition to the caveat provided regarding proper implementation of relying systems, the standard should also recognize that those relying systems may take advantage of identity authentication mechanisms outside the scope of FIPS 201 such as vascular pattern or other biometrics or PIN repositories. If the proper chain of trust can be validated, these authentication mechanisms are just as appropriate as card based ones.	Section 6.3 should be augmented with a statement to the effect, "Other authentication mechanisms that do not rely on data stored in (logical) or on (physical) the PIV card should be approved by the Agency as having similar levels of confidence as those present on the PIV card." Alternately, the statement could be, "Other authentication mechanisms that do not rely on data stored in (logical) or on (physical) the PIV card may be used but are outside the scope of this standard."	Resolved by AMAG-24.
AMAG-30	AMAG Technology	Adam Shane	E	40, 41	1241, 1244	4.2	In 4.2 mention is made of the "asymmetric key pair and cooresponding certificate", but in 4.2.2 this is described as the "private key and corresponding public key certificate". The latter is more accurate - only the public key has a certificate associated - and should be used throughout.	Change description to be consistent.	Accept.
AMAG-31	AMAG Technology	Adam Shane	T	54	1660, 1667	6.2.1, 6.2.1.1	Card authentication must be used prior to using PIN to activate a card, otherwise, PIN does not count as a trusted factor of authentication. Therefore, if the assumption that card authentication is performed in accordance with SP800-116, this authentication DOES provide protection against use of a revoked or expired card.	Section 6.2.1 and subsections should be reconsidered.	Declined. As noted in AMAG-27, there is no requirement (when operating over the contact interface) to authenticate the card prior to using the PIN to activate the card. As noted in SP 800-116, neither the PIN nor the card count as trusted factors of authentication in the BIO authentication mechanism. As there is no assumption that card authentication is performed as part of the BIO authentication mechanism, Section 6.2.1 correctly notes that the authentication mechanism does not protect against use of a revoked card.
AMAG-32	AMAG Technology	Adam Shane	T	55, 56	1706, 1726	6.2.3.1, 6.2.3.2	This section states that the reader validates the certificate. In the case of a transparent reader, it is not the reader but some other component of the system that is performing the validation.	This section is normative so will be interpreted that it must be implemented in this fashion. The statement should be updated to indicate that the system performs the validation, and not any specific component.	Resolved by revising the bullets to remove reference to who performs the action but specify what action must be performed or by replacing 'reader' with 'relying system' as appropriate. Follow the format used in BIO and BIO-A.
AMAG-33	AMAG Technology	Adam Shane	G				The standard is not at all clear about the intended use of the PIV Authentication key and Card Authentication Key and their associated public key certificates. When is it appropriate to use PAK or CAK for authentication? What are the requirements on a PIV issuance system and theh CA on revoking these certificates? For example, when does the CAK get revoked independently of the PAK? Does the PAK ever get revoked and not the CAK?	It is requested that NIST clearly define the use of these keys and authentication mechanisms.	Declined. FIPS 201-2 specifies the properties of each of these keys, including the levels of assurance associated with their corresponding authentication mechanisms, PKI-AUTH and PKI-CAK. The appropriate key to use for authentication in any given situation depends on the level of assurance required. Table 6-2 and table 6-3 provide guidance in this area. SP 800-116 also provides guidance in this area. It is outside the scope of FIPS 201-2 to attempt to provide an exhaustive list of reasons that a certificate may be revoked.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AT-1	AssureTec	Liz Galvin	G	viii	210	11	There is a large dichotomy between having rigorous, secure practices and policies for interoperability of the PIV system and reliance upon the issuer “that the individual in possession of the credential has been correctly identified.” Specific comments are made in reference to the individual statements below. The general comment is that there is very little emphasis on the ID Proofing process relative to authentication of “breeder” documents or validation of a “chain of custody” for the identity being claimed. The first step in building a “Chain of Trust” for the PIV is authentication of the primary source documents. The second is biometric linkage (typically facial match) of the applicant to the source document(s). The paper "*Stop Issuing Secure Credenetials to Imposters!" **http://www.fraudfreeid.com/Documents/StopIssuingSecureDocumentstoImposters.pdf*** provides a good background and references for this subject.	Therefore, Change the sentence/Phrase to read: assurence provided by the issuer of an identity credential has conducted an authentication of the source documents to verify that the individual in possessionof the PIV Credential has been correctly identified.	Resolved by OPM-3 and OSE-4.
AT-2	AssureTec	Liz Galvin	G	viii	210	11	Without guidelines for what constitutes an acceptable level of document checking and identity vetting, there can be no confidence in the identity of the bearer of the PIV. The claimed identity at issuance may not have a criminal record; have a confirmed credit history; and will pass a Tier 1 background check; and, yet, not belong to the applicant. It is widely recognized that individuals cannot be trained to recognize as authentic and unaltered the many combinations of documents accepted as proof of identity. (See the testimony of Michael Everitt, Unit Chief for FDL before the Senate Finance Committee August 2, 2006, ***http://www.c-spanvideo.org/program/FalseI*** specifically at the 00:26:52 mark).	Specify guidelines for use of machine readable authentication and a document examination.process. A certified level of fraudulent document detection training must be specified..	Resolved by adding the following sentence to Footnote 4 in Section 2.7: It is recommended that departments and agencies perform electronic verification of identity source documents, where possible.
AT-3	AssureTec	Liz Galvin	G	viii	210	11	Biometrics can confirm a link between a person and a physical document, event, or transaction. Once an identity has been verified and the link(s) to the person has been established, then biometrics can be used to “seal” the identity as belonging to that person. All of the subsequent identity management processes and the related security mechanisms serve only to protect the established identity and the rights/privileges associate with it and allow for interoperability amongst organizations when said identity is presented. Physical documents and the history of usage of an identity represent the linkage between the identity and the person claiming it.	Continuation of Recommendation 2	Noted. Aspects of this are already discussed in SP 800-63. This also represents the concept of Chain-of-trust.
AT-4	AssureTec	Liz Galvin	G	viii	210	11	There is no “assurance provided by the issuer of an identity credential that the individual in possession of the credential has been correctly identified,” unless this process meets a minimal set of common requirements amongst issuers. The total removal of FIPS 201-1 Appendix A removes all guidelines as to what is should be done to ID proof the applicant. The current status of SP 800 79-1 provides only the process requirements that the issuer must meet to qualify. Nowhere is there a set of measurement standards for the assessing the ID proofing and registration process.	Continuation of Recommendation 2	Noted. The text in Appendix A was informative which will be published as a separate NIST Interagency Report.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AT-5	AssureTec	Liz Galvin	G	viii	210	11	All data-only identity vetting fails to take into account the fact that the data sources being matched against are the very ones from which identity thieves reconstruct the personal information needed to go with stolen credit cards or account information. In this internet age a personal information data profile that is not readily accessible is mostly in the dreams of privacy advocates. Even electronic data verification with the issuer of the "original" ID does not mean that it is the ID that they issued which has been presented! People who attempt ID fraud using names that will not appear on a credit history check or fingerprints that will appear on a criminal background check are likely just plain incompetent and not a serious threat!	Continuation of Recommendation 2	Noted.
AT-6	AssureTec	Liz Galvin	G	viii	210	11	Therefore, it comes down to linking the authentication of documents and the chain of custody for the identity to the applicant who claims it is theirs. Please remember, examiners without the aid of machine authentication cannot be trained to recognize and reliably authenticate all of the many variations of source documents. There should be at least requirements for the use of systems such as the NAPHSIS EEVE for birth certificates, machine document authenticators, and "trust authority"-based systems which verify all properties (data, security, photo, and layout) of the source document against the issuers. Adjudicators should also be required to have accredited fraudulent document training to review documents that cannot be readily authenticated. In the case of foreign or difficult to authenticate source documents it is recommended that the document list be expanded to include any document relevant to the chain of custody for the adjudicator to consider in determining the probability that the claimed identity has belonged to the applicant for the last 15 years.	Continuation of Recommendation 2.	Resolved by AT-2.
AT-7	AssureTec	Liz Galvin	G	viii	210	11	An access methodology should be in place for referral to forensic experts at the ICE FDL or the FBI in cases where there are serious questions of document authenticity that cannot otherwise be resolved.	Any question of document authenticity which cannot be resolved will be referred to document experts within an apporved government agengy for further investigation.	Out of scope.
AT-8	AssureTec	Liz Galvin	G	1	239	1.2	Similar comment to Comment 1: unless the PIV "is issued based on sound criteria for verifying an individual … identity" then the overall security of the system is compromised. That criterion is not defined in FIPS 201-2. Nor is it defined in any referenced document!	See Recommendations 1 and 2.	Resolved by AT-1 and AT-2.
AT-9	AssureTec	Liz Galvin	G	1	239	1.2	Similar comment to Comment 1: unless the PIV "is issued based on sound criteria for verifying an individual … identity" then the overall security of the system is compromised. That criterion is not defined in FIPS 201-2. Nor is it defined in any referenced document!	See Recommendations 1 and 2.	Resolved by AT-1 and AT-2.
AT-10	AssureTec	Liz Galvin	G	5	351-369	2.1	If there exists an "official accreditation process" which specifies a " …sound criteria for verifying an individual employee's identity; (b)… **strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;** (c) **… rapidly authenticated electronically**; and (d) **… providers … reliability has been established…**," then it should be referenced.	Recommendation: Specifically, provide a definition of how the "two source documents" are to be determined as "genuine and not altered." By checking "watch lists" and other data sources for an identity that does not belong to the applicant serves no purpose. Hence, provide normative guidance as to how the control objective "Fraudulent identity source documents are not accepted as genuine and unaltered" is to be met.	Declined. Section 2.1 specifies the control objections, not the requirements for satisfying those objectives.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AT-11	AssureTec	Liz Galvin	T	9	479	2.7	SP 800-79 does not actually specify “an identity proofing and registration process.” The closest reference to this is in SP 800 79-1 Section 3.1 Introducing PCI Controls on Page 22 where it says “…identity-proof their applicants (i.e., use due diligence in validating the claimed identity of the applicant, using all documents provided by the applicant).” The “due diligence” criteria is not definitive and open for interpretation by each issuer.	Therefore, delete "[SP 800-79]" add the phase: "… accordance with this section…"	Resolved by replacing the bullet with: "The organization shall adopt and use an identity proofing and registration process that is approved in accordance with [SP 800-79]."
AT-12	AssureTec	Liz Galvin	T	9	489-526	2.7	Further clarification of “provide two forms of identity source documents in original form” is required. In support of the applicant appearance in person further requirements are needed. For example, the submission of original documents that must later be returned to the owner can be a serious logistic problem, as noted in the passport application process.	Recommend that all source documents be presented directly by the applicant and assessed for authenticity at that time. High-quality images should be captured as a part of the transaction audit process for later referral if necessary during adjudication. If there is any question of authenticity then the document should be retained for further forensic examination.	Noted. FIPS 201 requires in person appearance to identity proof. This level of detail is out of scope for FIPS 201. This level of detail is out of scope for FIPS 201.
AT-13	AssureTec	Liz Galvin	T	9	489-526	2.7	As noted in Comment 1, “individuals cannot be trained to recognize as authentic and unaltered the many combinations of documents accepted as proof of identity.” Even visual aids, such as the M-396 “Guide to U.S. Travel Documents” and the “ID Checkers Handbook” do not provide sufficient information to properly authenticate identity source documents. Very high high-quality driver’s license forgeries from companies like ID Chief are readily available and require specialized analysis for detection. Foreign passports are virtually impossible to authenticate without a smart document authenticator.	Add at the end of the section: Agencies will deploy source document authenticators that have the capability to detect all design characteristic, security features of the presented documents and compare these features to the source document's issuer, to the greatest extent possible. The agency will refer all suspected fraudulent documents to Law Enforcement for further investigation.	Resolved by AT-2. Requiring that all suspected fraudulent documents be referred to law enforcement for further investigation is out-of-scope for FIPS 201.
AT-14	AssureTec	Liz Galvin	T	9	489-526	2.7	Given the necessity of “real-time” forensic examination and document authentication of these source documents, additional normative guidance is needed. it is recommended that machine-based automated document authentication of all passports and federal and state government issued driver’s licenses and IDs be made a requirement of the identity proofing process.	Consitent with comment 12 above, recommend this alternative language: Agencies will deploy machine-based automated document authentication of all passports and federal and state government issued driver’s licenses and IDs be made a requirement of the identity proofing process.	Resolved by AT-2.
AT-15	AssureTec	Liz Galvin	G	10	530-537	2.7	The State Department has deployed document authenticators at all embassies and this facility should be a part of the process for identity proofing overseas workers for the federal government.	IBID Comments 12 and 13	Noted. The final paragraph of Section 2.7 states that for citizens of foreign countries who are working for the Federal government overseas "a process for identity proofing and registration must be established using a method approved by the U.S. Department of State’s Bureau of Diplomatic Security, except for employees under the command of a U.S. area military commander."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AT-16	AssureTec	Liz Galvin	T	11	561-564	2.8	During the issuance process there is no PIV card for comparison! I believe it was meant to say "…and compare the applicant with the facial images on the source documents." Given that it is very difficult to compare small ID photos.	Recommend add to the end of 564: Agencies will have a process which include the extraction of photo images from the source documents and magnification to a size suitable for easy comparison to the applicant and a recommendation that 1:1 facial matching between the applicant and the photo on the source document.	Declined. The text in lines 555 through 564 is referring to physically handing the newly created PIV Card to the applicant. Read in context, the final sentence is saying that (in the absence of a 1:1 biometric match) before handing the PIV Card to the applicant, an attendant shall compare the appearance of the person who has come to retrieve the card to the image on the card, in addition to checking the identity source documents that this person is required to present. Faces printed on paper and plastic are generally of poor quality, rendered more so by the scanning process. In any case some of the (secondary) identity source documents in section 2.7 do not contain a facial image.
AT-17	AssureTec	Liz Galvin	G	24-25	967-984	4.1.2	Inclusion of security features that rely upon human authentication is of primary value to the issuer and high-frequency examiners of the credential who will recognize the security feature and detect tampering. They are also very valuable any place where machine-based authentication is used. They can be trained to recognize security features from all issuers.	Insert at the end of Line 984 the following: where machine-based authentication is used, agencies will train the screeners/examiners to use these devices to detect security features, tampering defects and source document consistancy with the source document's issuer.	Declined. While machine-based authentication can be deployed, agencies should be deploying devices that can utilize the data stored electronically on the card (and the cryptographic keys on the card) rather than machines that attempt to authenticate the security features that are printed on the card.
AT-18	AssureTec	Liz Galvin	T	26	1030	4.1.4	It is recommended that the PIV card issuer rigorously maintain version control which is readily visible on the card. Changes in material suppliers, security features, printers, and layout could change the appearance of the card and potentially be confused as a forgery or alteration. It is further recommended, that "alignment marks" be included in opposing corners on all cards. This would provide more reliable decryption for any agency seeking to include data dependent layout. If specified on all cards then there would be no indication of possible inclusion of such data. Additionally it would increase the reliability of OCR or visible data for comparison against machine-readable data.	Add this comment within this section: Agencies will embed a version control indicator within the Magnetic Stripe or 2D barcode with a corresponding indicator printed on the face of the card. (Zone 4F?)	Declined. Federal Agencies and Department are free to use the 2D barcode, magnetic Strip and 4F to encode a version number. It is not necesarry to make visual versioning a requirement. Aligned by AT-17.
AT-19	AssureTec	Liz Galvin	T	59	1779- 1816	6.2.6	Because there will be many variations of security features and layout specifics, it is recommended that one or more common layout and security feature be specified, These should be present for any issuer and verifiable by any guard. Whenever viable, an alternate option for machine-based document authentication should be available to deal with the loss of central communication or in the unlikely event that the data encryption is compromised en masse. Possession of the PIV does not mean ownership. Therefore, imaging of the document would provide the ability to magnify the photo image for easy manual matching to the presenter. Capture of the data and document image will also provide an audit trail of the activity of the guard/access point in the event of any failure to the primary PIV system or as an alternative for some locations.	Recommend: that language be inserted to develop verification of PIV Cards from other agencies, expired PIV Cards, State-issued PIV-I Cards.	Declined. Verification of PIV cards issued by an agency or other agency is addressed through Section 6.2.1-6.2.5 authentication mechanisms. Verification of PIV-I card is out of scope. Also, see resolution of AT-17 and resolution to Cert-102 and Cert-115 in the disposition of comments to March 2011 draft FIPS 201.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
BAH-1	BAH	Rhonda Farrell	G	vii	170-176	8	Better to change the bullet style from (=) to some other visual character, as a (+) usually indicates some type of expansion is necessary - in this case, it is just itemizing items in a bulleted list	Bullet form (° •, etc.)	Declined in order to keep consistency with previous versions.
BAH-2	BAH	Rhonda Farrell	G	viii	210 - 215	11	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-3	BAH	Rhonda Farrell	E	xi, 1	N/A	first page after TOC	There is no page number, no title page, nor any indicator that it was intentionally left blank	remove or add page mumber and intentionally blank verbiage	Accept. The empty page will be removed.
BAH-4	BAH	Rhonda Farrell	E	vii, viii, 1	Line numbers are duplicated 202 - 233	1. Intro	The line numbers in the range 202-233 have been duplicated. 1st set of line are on pages vii-viii; and the second set of the same line numbers are on page 1.	Line numbers should be unique across the entire document.	Noted. The final version of the document will not include line numbers.
BAH-5	BAH	Rhonda Farrell	E	1	225-226	1.1	awkward last part of the sentence (… currently available and evolving).		Resolved by replacing: This Standard has been developed within the context and constraints of Federal law, regulations, and policy based on information processing technology currently available and evolving. With: This Standard has been developed within the context and constraints of Federal law, regulations, and policy based on currently available and evolving information processing technology.
BAH-6	BAH	Rhonda Farrell	E	viii	228-229	12	The acronym FISMA has already been defined on line 104-5 and can be used on line 228		Noted, however we believe that Federal Information Security Management Act of 2002 should be spelled out again here.
BAH-7	BAH	Rhonda Farrell	G	3-4	321-346	1.4	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-8	BAH	Rhonda Farrell	E	5	351-357	2.1	This information is completely redundant with data contained on pages 1-2, lines 237-242 (except for the inclusion of the HSPD12 para designator (3)	Perhaps pages 1-2 content can be paired back so that there is not complete redundancy	FIPS 201: Declined. Line 237-242 is the Scope section and the inclusion of the HSPD-12 control objectives are appropriate. Section 2.1, in turn, specifies how the control objectives can be met. A repeat of the control objectives, is appropriate.
BAH-9	BAH	Rhonda Farrell	G	5	360-378	2.1	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-10	BAH	Rhonda Farrell	G	6	387-290, 397-399, 401-403	2.3, 2.4	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-11	BAH	Rhonda Farrell	E	6	394	2.3	awkward first part of the sentence (fingerprint collection shall be conformant to the …)	Fingerprint collection shall conform to ….	Accept
BAH-12	BAH	Rhonda Farrell	E	6	407	2.4	awkward first part of the sentence (Biometric data collection shall be conformant to the …)	Biometric data collection shall conform to …)	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
BAH-13	BAH	Rhonda Farrell	E	7	418	2.5	may wish to append the acronym OCC-AUTH to the last portion of the sentence to make it clearer to the reader what is being referred to	OCC may be used to support card activation as described in Sectin 4.3.1. OCC-AUTH may be used to support cardholder authentication as described in Section 6.2.2.	Resolved by replacing: OCC may be used to support card activation as described in Section 4.3.1 and cardholder authentication as described in Section 6.2.2. with OCC may be used to support card activation as described in Section 4.3.1. OCC may also be used for cardholder authentication (OCC-AUTH) as described in Section 6.2.2.
BAH-14	BAH	Rhonda Farrell	E	7	421	2.6	the sentence refers to multimodal authentication, but readers may be more familiar with the term multifactor	Agencies may choose to collect iris biometrics as a second biometric to support multimodal (multifactor) authentication to improve…	Declined, the text refers to the use of different types of biometrics, such as fingerprint and iris recognition, and not multi-factor authentication.
BAH-15	BAH	Rhonda Farrell	G	7	425-430, 437-441	2.5, 2.6	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-16	BAH	Rhonda Farrell	G	8	442-452, 461-475	2.6	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-17	BAH	Rhonda Farrell	G	9	479-493	2.7	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-18	BAH	Rhonda Farrell	E	9	Footnote	2.7	For some reason the footnote is indented on lines 2-5 by 3 spaces		Resolved by removing indentation.
BAH-19	BAH	Rhonda Farrell	G	10	527-529	2.7	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-20	BAH	Rhonda Farrell	G	10-11	543-568	2.8	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-21	BAH	Rhonda Farrell	E	11	footnote	2.8.1	For some reason the footnote is indented on line 3 by 3 spaces		Resolved by removing indentation.
BAH-22	BAH	Rhonda Farrell	G	14	672-677, 697-703	2.9.3	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-23	BAH	Rhonda Farrell	G	15	714-726	2.9.4	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-24	BAH	Rhonda Farrell	G	16	751-755, 758-767	2.9.5	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-25	BAH	Rhonda Farrell	G	17-18	790-820	2.11	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-26	BAH	Rhonda Farrell	E	21	881-882	3.1.1	Awkward sentence - as 'something you have' is repeated twice	Better if the sentence removed the last (redundant) - "something you have", in order to read: … providing the card ("something you have") for cryptographic-key based authentication.	Resolved by CERT-4.
BAH-27	BAH	Rhonda Farrell	G	22-23	925-942	3.2	Same as comment #1	Same as comment #1	Resolved by BAH-1.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
BAH-28	BAH	Rhonda Farrell	G	24-26	970-975, 977-980, 987-1028	4.1.2-4.1.3	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-29	BAH	Rhonda Farrell	E	27	1053	4.1.4.1	It would be useful to have the relevant figure placed BEFORE the breakout explanatory text for all of the relevant fields	Move Figure 4-1 from page 32 to page 27 - before the field explanatory text is gone into in detail	Declined since this will be a major change to the layout of the document.
BAH-30	BAH	Rhonda Farrell	E	29	1087-1089	4.1.4.1	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-31	BAH	Rhonda Farrell	E	29	1100	4.1.4.2	It would be useful to have the relevant figure placed BEFORE the breakout explanatory text for all of the relevant fields	Move figure 4-6 from page 37 to page 29, before the field explanatory text is gone into in detail	Resolved by BAH-29.
BAH-32	BAH	Rhonda Farrell	E	29	1107	4.1.4.3	It would be useful to have the relevant figure placed BEFORE the breakout explanatory text for all of the relevant fields	Move figures 4-2, 4-3, 4-4, & 4-5 from pages 33 - 36 to page 29, before the field explanatory text is gone into in detail	Resolved by BAH-29.
BAH-33	BAH	Rhonda Farrell	E	31	1164	4.1.4.4	It would be useful to have the relevant figure placed BEFORE the breakout explanatory text for all of the relevant fields	Move figure 4-7 & 4-8 from pages 38 & 39 to page 31, before the field explanatory text is gone into in detail	Resolved by BAH-29.
BAH-34	BAH	Rhonda Farrell	E	38	1209	fig 4-7	Odd use of the term "English units". Ambiguous. Better if stated use US system units (feet and inches) versus metric.	Limit use of abbreviations. Use US system units (feet and inches) versus metric measures.	Resolved by replacing: Limit use of abbreviations. Use English units. With: Limit use of abbreviations. Use U.S. Customary units (e.g., feet and inches).
BAH-35	BAH	Rhonda Farrell	G	40	1228-1231	4.1.5	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-36	BAH	Rhonda Farrell	G	40-41	1239-1244, 1247-1248, 1251-1254,	4.2	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-37	BAH	Rhonda Farrell	G	42-44	1311-1323, 1334-1390	4.2.2	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-38	BAH	Rhonda Farrell	E	44	footnote 915)		For some reason the footnote is indented on line 2 by 3 spaces		Resolved by removing indentation.
BAH-39	BAH	Rhonda Farrell	G	45	1394-1387, 1399-1400, 1423-1425	4.2.3.1, 4.2.3.3	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-40	BAH	Rhonda Farrell	E	45	footnote (16)		For some reason the footnote (16) is indented on line 2 by 3 spaces & tfootnote (17) is not aligned correctly		Resolved by removing indentation.
BAH-41	BAH	Rhonda Farrell	E	45	1408	4.2.3.2	Need an 'a' added to the sentence content	The format for a CBEFF_HEADER is ….	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
BAH-42	BAH	Rhonda Farrell	E	46	1427	4.2.3.3	The pointer to the section for PIV Card activation is currently 4.3.1 - but this is pointing to the Activation by the cardholder only and not to activation by card management system. The sentence does not give the specific CONTEXT of the type of activation.	Point to the main PIV Card activation section (4.3) versus 4.3.1.	Declined. On-card biometric comparison will not be used to perform "activation by card management system," so it is appropriate for this sentence to refer specifically to Section 4.3.1.
BAH-43	BAH	Rhonda Farrell	G	45	1437-1444	4.2.4	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-44	BAH	Rhonda Farrell	E	49	1526	5.2.1	The list of PKI service providers is not contained at the high-level link given (http://www.idmanagement.gov)	Better if the websites exact URL was given as the top level URL does not have a linked page labeled PKI Service Providers and it is NOT intuitively obvious at which lower sub-page set the indicated data resides at.	Declined. The idmangement.gov web site may be reorganized at some point after FIPS 201-2 is issued, so pointing to the exact URL would not be appropriate as the URL may not be stable.
BAH-45	BAH	Rhonda Farrell	G	49	1530-1540	5.2.1	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-46	BAH	Rhonda Farrell	E	49	1534	5.2.1	Would be helpful if the reference to where the policies were located at were reiterated, as it differs from the Worksheet reference indicated in lines 1532-1534.	…either the id-fpki-common-hardware or id-fpki-common-High [COMMON] policy in the certficicate policies extention.	Resolved by changing the sentence to: ...either the id-fpki-common-hardware or id-fpki-common-High policy of [COMMON] in the certificate policies extension.
BAH-47	BAH	Rhonda Farrell	E	49	1538	footnote (17)	The footnote is missing the reference to where the certificate policies are stored.	…, or id-fpki-common-High policy in the certificate policies extension [COMMON].	Resolved by changing the sentence to: ...may assert the id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON] in the certificate policies extension.
BAH-48	BAH	Rhonda Farrell	E	50	1551-1552	5.4	Helpful if the referene to the policy locators were given.	…OID and the id-fpki-common-cardAuth OID, respectively [COMMON].	Resolved by changing the sentence to: Departments and agencies may assert department or agency-specific policy object identifiers (OIDs) in PIV Authentication Certificates and Card Authentication Certificates in addition to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth policy OID of [COMMON], respectively.
BAH-49	BAH	Rhonda Farrell	E	52	1601	6.1	The sentence references the fact that there are four assurance levels. However, those levels are not identified and defined until two paragraphs later - too long of a read between introduction and itemization - loses the reader	After the first two sentences in section 6.1 (1601-1603), insert data contained on lines 1617 - 1620 (4 assurance levels and their definitions). This way the flow is easier to read.	Declined. The levels of assurance are defined on the same page only few lines down.
BAH-50	BAH	Rhonda Farrell	E	52	1617-1620	6.1	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-51	BAH	Rhonda Farrell	E	53	footnote (22)		For some reason the footnote is indented on lines 2 & 3 by 3 spaces		Resolved by removing indentation.
BAH-52	BAH	Rhonda Farrell	G	54	1655-1662, 1665-1679	6.2.1, 6.2.1.1	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-53	BAH	Rhonda Farrell	E	53	footnote (23)		For some reason the footnote is indented on line 2 by 3 spaces		Resolved by removing indentation.
BAH-54	BAH	Rhonda Farrell	G	55	1696-1698	6.2.2	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-55	BAH	Rhonda Farrell	E	55	footnote (24)		For some reason the footnote is indented on line 2 by 3 spaces		Resolved by removing indentation.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
BAH-56	BAH	Rhonda Farrell	G	55-59	1705-1716, 1718-1722, 1725-1734, 1736-1739, 1744-1753, 1756-1759, 1764-1769, 1771-1774, 1783-1790, 1799-1810, 1812-1816	6.2.3.1-6.2.6	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-57	BAH	Rhonda Farrell	E	56	footnote (25)	6.2.3.2	For some reason the footnote is indented on line 2 by 3 spaces		Resolved by removing indentation.
BAH-58	BAH	Rhonda Farrell	E	58	1781-1794	6.2.6	It would be very helpful to reference a set of figure(s) that showed what the various PIV card fields are: ZoneN	Add as necessary - Figures 4-1 thru 4-8	Declined. It might confuse the reader to point out a zone in one figure when the same zone appears in several other figures.
BAH-59	BAH	Rhonda Farrell	E	59	1825-1826	6.3	Would be helpful to differentiate why two tables are necessary to explain the assurance levels. (one is logical and one is physical access).	Adequately designed and implemented relying systems can achieve the PIV Card authentication assurance levels stated in Tables 6-2 (physical access) and 6-3 (logical access).	Accept to revise the sentence as proposed.
BAH-60	BAH	Rhonda Farrell	G	61	1876-1879, 1882-1885	A.1	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-61	BAH	Rhonda Farrell	E	61	1875	A.1	The four major accreditation topics identified in [SP 800-79] actually have FIPS 201-1 as their source. It would be helpful to have the source spec listed as the base requirements are what require that a set of controls be put into place to address them.	Rather confusing to the reader when trying to source the actual topic areas. Better if FIPS202-1 was mentioned.	Declined. The four phases in SP 800-79 as well as the Accreditation Topics are part of the Assessment methodology NIST has proposed to assess the capabilities of the PIV Card Issuers (PCI) to issue cards according to FIPS 201 requirements. The Assessment methodology by itself is independent of FIPS 201 requirements. It is the set of controls that have been assessed that should have as their reference the requirements in FIPS 201 and its revisions. Hence the controls assessed will be updated in SP 800-79 to reflect the new/modified requirements of FIPS 201-2.
BAH-62	BAH	Rhonda Farrell	E	61	1880-1881	A.1	The four phases do not have a corresponding reference. In actuality they are within the [SP 800-79] document.	The entire spectrum of activities in the PCI accreditation methodology is divided into the following four phases [SP 800-79]:	Resolved by BAH-61.
BAH-63	BAH	Rhonda Farrell	E	62	1904	A.2	There is an inconsistenly applied reference - SP 800-70. It appears that when the contents of an external document are spoken to, the doc reference is placed within [ ]. In one case, the external document is missing the [ ] and it appears that they should be added.	… mandatory for issuing PCI accreditation using SP 800-79.	Resolved by placing brackets around "SP 800-79" at the end of Appendix A.2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
BAH-64	BAH	Rhonda Farrell	E	63	1939-1942	B.1	There is limited backward xref to the original section which defined PIV objects and no forward reference to the eContent Types or PIV Attributes or PIV Extended Key usage	In Chapter 4 (and other sections) it would be useful to have some forward pointers to this Appendix if further details are required (this would show that the appendix content adds value to the reader in some manner).	Noted. There are already forward references to Appendix B in Sections 4.2.1 and 4.2.3.2 with respect to the id-PIV-content-signing OID. There are no forward references to the eContent types since the details of the CMS signatures, which is where the eContent types appear, have been removed from the July 2012 Draft FIPS 201-2 as per Cert-75 and Cert-92 in the disposition of comments for the March 2011 Draft FIPS 201-2.
BAH-65	BAH	Rhonda Farrell	G	63	1950-1953	B.2	Same as comment #1	Same as comment #1	Resolved by BAH-1.
BAH-66	BAH	Rhonda Farrell	E	63-64	1944	B.2	There is no forward reference to the B.2 Appendix, either via the object identifier name (id-piv-NACI) or through the OID.	Content was included in an Appendix for a reason, but there is no references from earlier sections which call out this appendix. Should include some forward references if at all possible.	Resolved by changing the sentence in Section 4.2.2, beginning on Line 1345, to read: The PIV Authentication certificate shall include a PIV NACI indicator (background investigation indicator) extension (see Appendix B.2); this non-critical extension indicates the status of the subject's background investigation at the time of card issuance.
BAH-67	BAH	Rhonda Farrell	E	69	2119-2197	C.2	There are some acronyms which are used in the prior sections which are not defined in this section: FICAM, PKI-CAK, OCC_AUTH, SYM-CAK, ATO, DATO, ASN.1	Please add the definitions so that the acronym list will be complete.	Resolved by adding the following to Appendix C.2: ASN.1 - Abstract Syntax Notation One ATO – Authorization to Operate DATO – Denial of Authorization to Operate FICAM – Federal Identity, Credential, and Access Management Note, PKI-CAK, OCC-AUTH, and SYM-CAK are not added to Appendix C.2 as these are names for authentication mechanisms, not acronyms.
BAH-68	BAH	Rhonda Farrell	E	72	2219	Appendix D	The [FISMA] reference is not currently being referenced in the text. The acronym is used, and explained, but the reference indicator is missing (see lines 105, 228-229 [first set of those line numbers]).	Please add reference indicator within the body of the document.	Resolved by changing Section 12 of the Announcement to read: As per the Federal Information Security Management Act of 2002 [FISMA], waivers to Federal Information Processing Standards are not allowed.
BAH-69	BAH	Rhonda Farrell	E	73	2241	Appendix D	The [NISTIR7123] reference is not currently being referenced in the text. Additionally, neither the acronym nor the doc title is being referenced within the text.	Please add reference indicator, acronym, and reference title to the body of the doc.	Resolved by removing [NISTIR7123] from Appendix D.
BAH-70	BAH	Rhonda Farrell	E	73	2270, 2004	Appendix D	The [RFC 5280] reference on page 2004 should not have a space between the C and the 5 (to make it consistent with other reference indicators).	Please add reference indicator within the body of the document.	Resolved by removing space from "[RFC 5280]" on line 2004 and from "[RFC 2560]" on line 2076.
BAH-71	BAH	Rhonda Farrell	E	73	2272	Appendix D	Pages 1275-1276 are missing the [RFC5652] reference which is defined on page 73, line 2272.	Please add reference indicator within the body of the document.	Declined. The referenced text states that "The asymmetric signature data element of the CHUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as specified in [SP 800-73]." While CMS is defined in RFC 5652, SP 800-73 is the correct reference here, since SP 800-73 will specify the requirements for the CMS external digital signature for the CHUID. The text in SP 800-73 specifying the requirements will reference RFC 5652.
BAH-72	BAH	Rhonda Farrell	E	74	2279-2280	Appendix D	The reference [SP 800-59] is not mentioned in the doc at all.	Please add reference indicator within the body of the document.	Resolved by changing the first sentence of Section 6 of the Announcement to read: This Standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems, except for "national security systems" as defined by 44 U.S.C. 3542(b)(2) [SP 800-59].

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
BAH-73	BAH	Rhonda Farrell	E	31	1166	4.1.4.4	The sentence references ISO7811, but looking at the references contained within Appendix D, this particual reference is missing an entry.	Please add reference entry.	Accept. Add reference in Appendix D.
BAH-74	BAH	Rhonda Farrell	E	40	1217	4.1.5	There is a reference made to IEC 61966, but that reference is not contained within Appendix D. Also, it is formattted incorrectly, there should be no space between the IEC and the 61966, components (if wish to be compliant with all of the other reference syntax).	Please add reference entry.	Accept. Add reference in Appendix D and to remove space from reference.
BAH-75	BAH	Rhonda Farrell	E	47	1490	4.4.3	There is no entry in Appendix D with the entry ISOIEC 24727.	Please add reference entry.	Accept. Add reference in Appendix D
CB-1	Codebench, Inc.	Bob Fontana	T	42	1278	4.2.1	There needs to be a specification for the validity period of content signing certificates. FIPS 201-1 does not specify the validity period for content signing certificates. As a result, content signing certificates expired before the CHUID's expiration date. Relying parties must choose to (a) treat the PIV card as invalid due to an expired content signing certificate or (b) ignore the notAfter date of the content signing certificate. Because the content signing certificate is a X.509 certificate, the corrrect way to validate it is to use the same PD-VAL algorithm as is used to validate the other certificates on the card. Therefore, ignoring the notAfter date is not viable.	Add a requirement that the notAfter date of any content signing certificate must be greater than or equal to the notAfter date of the PIV Authentication certificate or the CHUID expiration date, whichever is later.	Resolved by adding sentences to Sections 4.2.1 and 4.2.3.2 that say: "The content signing certificate on a valid PIV Card (one that is neither expired nor revoked) shall not be expired." FIPS 201 states that the expiration of the PIV Authentication certificate shall be no later than the expiration date of the card, and that the expiration date in the CHUID shall indicate when the card expires. So, the expiration date of the PIV Authentication certificate can never be later than the CHUID expiration date. Requiring that the notAfter date of any content signing certificate be greater than or equal to the expiration date of the card would be overly constraining as the signed data on a PIV Card (CHUID, biometrics, security object) may be re-signed during the card's lifetime via a post issuance update.
CDC-1	CDC/NIOSH	Bill Brinkley	E	52, 59	1626, 1855	6.1.1, 6.3.2	CDC NIOSH has concerns with the notional linkage between E-Auth Level 2 and PKI-CAK for Remote/Network System Access via the tables 6-1 and 6-3. NIST Special Publication 800-63-1, Electronic Authentication Guideline, states in Section 8.3.2.3 that E-Auth "Level 3 assurance may be satisfied by client authenticated TLS (implemented in all modern browsers), with Claimants who have public key certificates. Other protocols with similar properties may also be used."		Noted. The Card Authentication key on the PIV Card may be used even without activating the card (i.e., without cardholder authentication). Thus the PKI-CAK authentication mechanism only one-factor ("something you have") authentication. As stated in the Executive Summary of SP 800-63-1, for E-Auth Level 3 "At least two factors of authentication are required." The PIV Authentication key (used in the PKI-AUTH authentication mechanism) may only be used after the cardholder has authenticated to the card. This results in two-factor authentication and thus a higher level of assurance.
CERT-1	CertiPath	Judith Spencer	E	vi	137	6	This references *the contiguous United States* which would, by definition, exclude Alaska and Hawaii - was this intentional?	None - just bringing NIST's attention to the use of the term contiguous and ensuring this was the intent.	Noted.
CERT-2	CertiPath	Judith Spencer	E	12	582-598	2.8.2	Who determines the definition of 'short' in this context. OPM? The agency? Can it be 6 months, a year, two years?	Recommend NIST provide some definition of "short" or at least who is authoritative for determining this.	Resolved by OPM-28.
CERT-3	CertiPath	Judith Spencer	T	15	721-733	2.9.4	For an unattended kiosk, the use of a biometric should be restricted to on-card or specify chain of trust record. The card biometric is not accessible for off-card match without presentation of the PIN, and the kiosk will likely not have the ability to withhold the card if the match fails after pin reset as in the in-person scenario.	Recommend the 2nd bullet be revised to indicate on-card biometric match or chain of trust record match.	Accept.
CERT-4	CertiPath	Judith Spencer	E	21	881-882	3.1.1	The parenthetical *("something you have")* appears twice.	Remove second incidence of *(something you have)*.	Accept.
CERT-5	CertiPath	Judith Spencer	T	47	1462-1469	4.3.2	Is Card Management System Activation invoked for unattended PIN reset? (See comment 3 above). If so, it should say so here. And perhaps be included in Section 2.9.4.	Include PIN reset if it applies here.	Declined. As described in Section 3.2.3 of SP 800-73-3 Part 2, the PIN is reset using the RESET RETRY COUNTER card command, which does not require card activation by the card management system.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
CERT-6	CertiPath	Judith Spencer	T	54	1680-1683	6.2.1.2	The statement here suggests BIO and BIO-A are the same.	Recommend a statement be made that summarizes the advantages of BIO-A (witness to live capture etc.).	Resolved by replacing "This authentication mechanism is the same as the unattended biometrics (BIO) authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder." with "In this higher assurance variant, an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder. Otherwise, the steps for this authentication mechanism are the same as for the unattended biometrics (BIO) authentication mechanism."
CERT-7	CertiPath	Jeff Barry	E	43	1313-1314	4.2.2	Text is a bit confusing… "The asymmetric Card Authentication key is a mandatory private key that supports"	Recommend NIST make the language wording consistent across keys for this section: "The Card Authentication key is a mandatory asymmetric private key that supports"	Declined. A PIV Card may optionally have a symmetric (secret) Card Authentication key in addition to the mandatory asymmetric Card Authentication key. Thus "asymmetric" needs to be part of the key's name in order to distinguish it from the symmetric Card Authentication key.
CERT-8	CertiPath	Jeff Barry	E	43	1317-1319	4.2.2	With the digital signature and key management keys now mandatory when a government email address has been given, the language here should reflect that.	Recommend NIST make a change to the digital signature and ke managemet key to include the statement: ". The X key is mandatory if the cardholder has been issued a government email address, otherwise this key is optional."	Resolved by changing the relevant bullets as follows: + The digital signature key is an asymmetric private key supporting document signing, and it is mandatory, unless the cardholder does not have a government-issued email account at the time of credential issuance. + The key management key is an asymmetric private key supporting key establishment and transport, and it is mandatory, unless the cardholder does not have a government-issued email account at the time of credential issuance. Optionally, up to twenty retired key management keys may also be stored on the PIV Card.
CERT-9	CertiPath	Steve Howard	T	vii	181	8	This lists 800-73 and 800-78 as sufficient and complete definintion of PIV card. Must also have 800-76 to complete the definition of what goes on the card.	Add [800-76] to this sentence.	Declined. The NIST PIV Validation Program validates the PIV card's interface (APDUs) and PIV Middleware API. Both interfaces are tested using the specifications in SP 800-73 and SP 800-78. SP 800-76, however, is tested as part of GSA's validation program for personalization products. See Appendix A for futher details
CERT-10	CertiPath	Steve Howard	T	9	502	2.7	PIV-I credentials meet LOA 4 identity vetting.	Consider adding PIV-I as a valid document.	Declined. As per Cert-12 in the disposition of comments for the March 2011 draft of FIPS 201-2, PIV-I cards will not be listed as acceptable forms of identity source documents since they are not guaranteed to be Federal or State government issued forms of identification.
CERT-11	CertiPath	Steve Howard	T	14	672-673	2.9.2	This is an open ended requirement on relying parties who may have had the UUID/FASC-N entered into their systems. There is no mechanism to "revoke the card" required in this standard. Particularly, a revocation mechanism which is independent of "revoke the certificates". Is this purely something the issuer does within their IdM/CIS?	Recommend revoke the card is represented by the revocation of the CAK.	Resolved by AMAG-15.
CERT-12	CertiPath	Steve Howard	T	16	759-760	2.9.5	"revoke the card" issue	see prior comment for lines 672-673	Resolved by AMAG-15.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
CERT-13	CertiPath	Steve Howard	T	41	1264	4.2	If BIO-OnCardComparison is used without any crypto response, it is a YES Machine. Any card or attacking device could set a flag saying "I did BIO-OCC successfully".	Remove reference to "third category"	Declined. The fingerprint templates for on-card comparison may be used by the card to prove the identity of the cardholder to an external system (see Section 6.2.2). As per Section 6.2.2, the response from the card includes information that allows the reader to authenticate the card which effectively mitigates the YES machine threat. This is specified in further detail in Appendix B.1.4 of the initial draft of SP 800-73-4 Part 1.
CERT-14	CertiPath	Steve Howard	T	42	1280-1281	4.2.1	FPKIPA is considering a contentSigning policy OID for federal PIV issuance systems.	Must resolve if this is approved and then should refence the contentSigning OID only. Strongly recommend refering to FedPKI and Profiles in place of specifically listing them here.	Resolved by FPKI-3.
CERT-15	CertiPath	Steve Howard	T	45	1414-1415	4.2.3.2	FPKIPA is considering a contentSigning policy OID for federal PIV issuance systems.	Must resolve if this is approved and then should refence the contentSigning OID only. Strongly recommend refering to FedPKI and Profiles in place of specifically listing them here.	Resolved by FPKI-3.
CERT-16	CertiPath	Steve Howard	T	50	1562-1565	5.5	What mechanism says the card itself is revoked? Here again is the confusion that if the authentication certs are revoked, then the card is revoked. The sentence says a card is not revoked if the certs are revoked. The last sentence says presence of valid certs means not revoked. What is the mechanism for revocation of the card itself?	Recommend revoke the card is represented by the revocation of the CAK.	Resolved by AMAG-15.
CERT-17	CertiPath	Steve Howard	T	54	1657-1658	6.2.1	The PIN verification as a factor of authentication is in conflict with SP800-116 and the FICAM PIV in E-PACS guidance documents. The PIN itself is not an independently verified factor by the system. Only the Bio is actually verified by the system. Hence PIN does not count.	Align FIPS 201-2 with SP800-116 and PIV in E-PACS documents. They are more accurate and provide a more secure implementation. NOTE: 6.2.1.2 _can_ claim PIN, as it is observed.	Declined. The statement does not say that PIN verification counts as a factor of authentication. It only states that the PIN is required to use an unaltered card. Unlike for some of the other authentication mechanisms, there is no statement that the BIO authentication mechanism is resistant to credential forgery.
CERT-18	CertiPath	Steve Howard	T	60	1841-1848	6.3.1	The authentication modes offered by a PIV card for PACS here are incomplete and misleading. They are also in conflict with SP800-116 and the FICAM PIV in E-PACS. These two documents are much stronger and more accurate. It is CRITICAL that this be corrected in 201-2 for the success of enterprise wide PACS for the fed.	Use the table on adjacent page (columns J-L). It shows ALL modes of PIV authentication, their number of factors, and confidence. Note this is consistent in Strength of Auth achieved by factors of authentication. These are fully consistent with how a PIV card operates and what FIPS 201-2 is specifying for the main modes of authentication.	Declined. SP 800-63 is the basis for assurance levels assigned to the PIV authentication mechanisms. As per SP 800-63, PKI-AUTH satisfies the requirements for VERY HIGH assurance level. FIPS 201-2 notes that Table 6-2 defines the minimum requirement for each assurance level. FIPS 201-2 Section 6.3.1, says “Moreover, the authentication mechanisms in Table 6-2 can be combined to achieve higher assurance levels.” See also DoD-65 in the disposition of comment of the March 2011 Draft.
CM-1	Private Citizen	Private Citizen	T	46	1457 - 1459	4.3.1	Regarding the statement, "The PIV Card shall include mechanisms to block activation of the card after a number of consectuve failed activation attempts.", does NIST anticipate providing/specifying a security object that is similar to, but separate from the PIN Unblocking Key (PUK)/Retry Counter approach described in SP 800-73 (Part II, section 3.2.3), to support this technical implementation challenge? For example, while three (3) attempts may be appropriate for PIN entry, that may not be appropriate for presentation of fingerprint biometrics for OCC. (I recognize that the Second Draft of SP 800-76-2, section 10.5 provides some guidance/justification along these lines reference agency consideration of false rejection performance).	Consider adding a sentence that says something along the lines of "The number of allowable consecutive failled activation attempts may vary by authentication mechanism and will be determined by agency specific policy, and in accordance with NIST SPs 800-73, 800-76, etc.." Next, update NIST SP 800-73 accordingly.	Resolved by adding the following text to the end of the 1st paragraph of Section 4.3.1: "The number of allowable consecutive failed activation attempts may vary by activation mechanism."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
CS-1	Private	C&S	E & T	vi	137	6	NIST has changed the terminology from "PIV Credential" to "PIV Card." "PIV Card" is a misnomer and "credential" (i.e., something that gives confidence) best describes the PIV device/token. Further, the term moniker "credential" provides heightened sense of responsibility for *federal* property. The term *card* places it in the same category as one might use for a *business card*. Lines 186-187 reflect the proper reference to the PIV Credential.	Where applicable, delete all changes to the term "PIV Card" and restore the term/reference of "PIV Credential."	Declined. The item being referenced here is a card, so it is properly referred to as a PIV Card. The term credential is more appropriately used to refer to the information on the PIV Card that may be used to authenticate the cardholder.
CS-2	Private	C&S	T	3	287	1.3.5.	Verbiage discusses "PIV Cards" which conflicts with the terminology (i.e., PIV Card) used in line 137 supra.	Restore the term/reference of "PIV Credential" in line 137 (et alia)	Resolved by CS-1.
CS-3	Private	C&S	T	5	360, 362, 373, 374, 377	2.1.	Verbiage discusses "PIV Cards" which conflicts with the terminology (i.e., PIV Card) used in line 137 supra.	Restore the term/reference of "PIV Credential" in line 137 (et alia)	Resolved by CS-1.
CS-4	Private	C&S	T	5	364 (& 487)	2.1.	If an NCHC is completed, a PIV Credential can be issued. However, if there are issues (i.e., a hit) on the NCHC, the verbiage in this section authorizes an agency to issue a PIV Credential without reviewing/considering the results of the NCHC inquiry. NCHC's may reveal an individual has been entered into the AFIS for issues that may preclude the issuance of a PIV Credential. The verbiage provided enables agencies to issue PIV Credentials upon the completion of an NCHC check; however, more precise guidance needs to be provided that will preclude issuance of a PIV Credential where an NCHC check may reveal disqualifying information.	A credential is issued only after National Agency Check with Written Inquiries (NACI) (or equivalent or higher) or Tier 1 or higher federal background investigation is initiated and the Federal Bureau of Investigation (FBI) National Criminal History Check (NCHC) portion of the background investigation is returned with no issues found, or issues returned are adjudged to not disqualify the individual from receipt of the credential.	Declined. The referenced text was written to align with OMB Memorandum M-05-24.
CS-5	Private	C&S	T	7-8	431-475	2.6	The section promotes & encourages the capture & long-term storage of biometric PII data (e.g., Extended Enrollment; Reissuance; Interagency transfer (L-461-475)). Storage or biometrics beyond that which is necessary (i.e., held in IdMS until PIV Credential is issued), presents an unwarranted retention of irrevocable PII data should it be compromised by crackers who penetrate USG networks/DBs. Theses and white papers reveal how fingerprints may be reconstructed from fingerprint templates. The long-term retention of PII biometrics serves no purpose other than convenience for the issuer. Current language authorizes the interagency transference of “chain-of-trust” information; however, this is contrary to OPM hiring (EOD) practices that requires the recapture of I-9 data whenever a federal employee changes agencies.	Update language to prohibit long-term retention of biometric data, allowing retention only for issuance purposes.	Declined. As can be seen from other comments that were submitted on Revised Draft FIPS 201-2 (CERT-3, DoD-11, DoD-16, SCA-25, XTEC-9, XTEC-22), there is significant interest in being able to use biometric data that is stored in the chain-of-trust to perform various PIV maintenance operations. While commenter states that retention of biometrics "serves no purpose other than convenience of the issuer," efficiency is a stated goal of HSPD-12, with which FIPS 201 must comply. It has been noted by many people who have commented on FIPS 201, that there are a lot of federal employees who do not work close by to an issuance station, and for whom trips to issuance stations are costly and time consuming. Maintenance of biometric data in a chain-of-trust permits the number of trips to be reduced. For example, a new card may be issued with only one in person visit, rather than one visit to collect biometric data and a second trip to collect the card. FIPS 201 cannot ignore these efficiency issues.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
CS-6	Private	C&S	T	9-10	489-537	2.7	In January 2013, all States are to comply with the REAL ID Act of 2005 (the Act), however, issues concerning ID documentation and compliance with the Act are not being addressed within FIPS-201-2. There is no national-level guidance on how federal agencies should address identification documentation (e.g., driver's licenses, et alia) to determine if they comply with the Act, any grace period for ID documentation issued prior to mandated compliance date(s), nor how a federal agency (or entities that issue PIV-Interoperable credentials) are to determine which States have been determined to be in compliance with the Act, or which have been granted extensions, et alia. The silence on this issue is deafening. Declining to address the Act based on Form I-9 does not address the requirements of the statute. As a mandate for federal executive depts./agencies, and a model for entities issuing PIV-I credentials, the Act must be addressed to ensure approved guidance to the executive branch on adherence to the Act. Since FIPS-201-2 is not anticipated to be promulgated until early 2013, this issue is ripe for addressing in this document to ensure a uniformed approach to verifying and compliance with the Act.		Declined because it is out of scope. The commenter appears to be asking NIST to address issues that are under the purview of the Department of Homeland Security (http://www.dhs.gov/secure-drivers-licenses).
CS-7	Private	C&S	T	9	503-504	2.7	Provide clarification for ". . . cannot be of the same type as the primary identity source document." Current statement is ambiguous.	The secondary identity source document may be from the list above, but may not be of the same as the primary identity source document.	Resolved by adding the following footnote to clarify 'same type'. "For example, if the primary source document is a foreign passport (e.g., Italy), the secondary source document should not be another foreign passport (e.g., France)."
CS-8	Private	C&S	T	10	525	2.7	Documentation such as passport (or WHTI documentation) are now needed to cross the US/CAN border. Acceptance of Canadian driver's license should be removed from approved documents for PIV issuance.	Delete L-525	Declined. The requirement to have a passport to cross the U.S/Canadian border does not make a Canadian driver's license any less valid as a secondary identity source document.
CS-9	Private	C&S	T	10	541	2.8	Approval should be under the purview of the PIV Senior Agency Official (SAO - as identified by NIST SP 800-79) who is (or should be) appointed by the Head or Deputy for an agency/department. Involvement of such high level officials is excessive.	The issuance process used when issuing credentials shall be accredited by the department as satisfying the requirements below and approved in writing by Federal department or agency Senior Agency Official (SAO) for the PIV Credential Issuance (PCI) process.	Resolved by DoD-10.
CS-10	Private	C&S	T	11	561-64	2.8	IF biometrics cannnot be matched at issuance, the attending operator must make a notation in the chain-of-trust record before the credential is issued. The notation must include what documentation was inspected (a scanned copy of the documentation (electronically verified as a valid credential/document) should be maintained in the cardholder's PCI files (chain-of-trust) to guarantee/bolster reliability of an individual's identity).		Declined. FIPS 201 does not specify mandatory requirements for chain-of-trust since it is an optional feature. However, it is possible for agencies to implement measures as the comment suggests. Note that Section 2.6 describes enrollment data records that enable measures as suggested by the comment.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
CS-11	Private	C&S	T	11	572-80	2.8.1	Example given in IRS Manual suggests that agencies may decide to issue PIV Credentials based on long-term or habitual use of a pseudonym (see §10.5.7.1, ¶3.A. & B. of IRS Manl). In L-576, the term harassment may include someone desiring not to use their given name for personal versus professional reasons. (e.g., someone doesn't like being the name Horatio but prefers to use the name "Buzz" but use of Horatio doesn't warrant possible physical harm, or endangerment to the individual). As written, agencies will dilute the authenticity of the PIV Credential by installing lax procedures/approval processes that allow individuals to use familiar or preferred nicknames/monikers versus source/feeder document identities. Footnote 5 should be deleted because it may cause confusion (not the grandfathering of pseudonyms).	In limited circumstances, Federal employees and contractors are permitted to use pseudonyms during the performance of their official duties with the approval of their employing agency. If an agency determines that use of a pseudonym is necessary to protect an employee or contractor from physical harm or endangerment, the agency may, after establishing formal policy guidance identifying a reasonable expectation of physical harm or endangerment is possible if a pseudonym is not used, authorize the issuance of a PIV Card to the employee or contractor using the agency-approved pseudonym. The issuance of a PIV Credential using an authorized pseudonym shall follow the procedures in Section 2.8, PIV Card Issuance Requirements, except that the card issuer must receive satisfactory evidence that the pseudonym is authorized by the agency. Nicknames, or familiar monikers cannot constitute the need for use a pseudonym on a PIV Credential.	Declined. The term harassment cannot reasonably be interpreted to justify the authorization for the use of a pseudonym based on personal preference. There is nothing in the IRS Manual that suggests that the use of a pseudonym may be authorized based on long-term or habitual use. While §10.5.7.1, ¶3.A notes that Section 3706 of RRA 98 permits the continued use of pseudonyms by those who used them before the enactment of the statute, that is a clearly limited exception that was permitted by statute. Those not "grandfathered" in under the statute must provide adequate justification (see see §10.5.7.1, ¶3.B.), where adequate justification is defined in §10.5.7.2.5. If FIPS 201-2 were to limit the use of pseudonyms to cases in which it "is necessary to protect an employee or contractor from physical harm or endangerment," it would preclude legitimate uses of pseudonyms that are currently permitted by Section 10.5.7 of the Internal Revenue Service Manual.
CS-12	Private	C&S	T	12	581-98	2.8.2	See comment CS-5 supra: This § encourages the long-term retention of irrevocable PII data. Because a new card must be issued whenever there is a change in status (e.g., contractor to fed, or fed to contractor, et cetera), the issuance process should be re-initiated to ensure proper sponsorship, and to recapture current biometric (e.g., facial/fingerprint template) data.	Delete § 2.8.2	Resolved by CS-5.
CS-13	Private	C&S	T	12	620-21	2.9.1	See Comment CS-5: The Chain of redential (On Card Comparison) to renew a PIV Credential,. If the PIV Cred has been lost or cannot be used to perform the 1:1 biometric match, then the initial isuance process should be followed (i.e., presentation of documentation presented in § 2.7, recapture of biometrics (not necessarly resubmissoin to NCHC or OPM).	Update this § to preclude the use of a long-term biometric DB for 1:1 biometric comparison. Use of OCC should be only acceptable appraoch for biometric matching.	Resolved by CS-5.
CS-14	Private	C&S	T	13	658-59	2.9.2	See Comment CS-5: Remove capability for maintaining a long-term DB for biometric records		Resolved by CS-5.
CS-15	Private	C&S	T	14	679	2.9.2	In the event of a lost, stolen, or compromised credential, recation should take place as soon as possible.	Change to read: In the case of a lost, stolen, or compromised credential, normal revocations procedures shall be completed as soon as possible, but no later than 18 hours from receipt of notification.	Declined. While agencies should complete normal revocation procedures as soon as possible, an "as soon as possible" requirement cannot be imposed as there is no clear means of determining whether an agency is satisfying that requirement.
CS-16	Private	C&S	T	15	716	2.9.4	See Comment CS-5: OCC should be the only procedure for biometric match.	Delete "off-card" biometric match authorization	Declined. Support for OCC is optional, and so FIPS 201-2 must continue to support PIN resets even for cards that do not support OCC.
CS-17	Private	C&S	T	16	753	2.9.5	A contractor may require access to federal buildings or systems; however, those buildings/systems may not be under the auspices of the Credential issuer.	Change to read: a contractor changes positions and no longer needs access to Federal buildings or systems under the auspices of the Credential issuer;	Declined. As long as the contractor is eligible to hold a PIV Card, there is no requirement for a PIV Card issued by one agency to be terminated, with a new PIV Card then being issued by another agency. So, it would be incorrect to say that the PIV Card shall be terminated in this case.
CS-18	Private	C&S	E	16	755	2.9.5	Issue is already addressed in L-753.	Delete L-755	Declined. Line 753 only applies to contractors, whereas Line 755 applies to all cardholders. Also, note that a cardholder passing away is different from a cardholder changing positions.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
CS-19	Private	C&S	T	31	1164-1190	4.1.4.4	Save the zones where mandatory data is required (ref § 4.1.4.2.), suggest allowing Depts/Agencies to place whatever data they desire on the back of the card (as long as it doesn't damage the ICC), wherever they desire. This section should provide suggestions, but not mandate specific zones where the data - if used - must be placed.		Declined. FIPS 201-2 is a standard and it specifies requirements for mandatory and optional components for PIV card. Placement for some optional components are dictated by standards (e.g., Magnetic Stripes) while other areas provide flexibility for agency-specific text (e.g., zones 9B and 10B).
CS-20	Private	C&S	T	41	1253	4.2	Meaning unclear. If a CAK is required for Phyiscal Access Apps/Control, then this cannot be an "optional" item.	NIST needs to specify physical access control criterion if CAK is not required.	Declined. Line 1253 states that a symmetric Card Authentication key may be used to support physical access applications, not that it is required.
DAON-1	Daon	CT	G	16	772	2.1	We anxiously await the draft of SP 800-157. (As you may expect, it is difficult to review this new derived credential capability without further detail.) Same for 800-156.	None.	Noted.
DAON-2	Daon	CT	T	27	1057	4.1.4.1	Should there be a requirement for the printed name to match the DN in the cert? This can sometimes cause confusion when they do not match.	Consider this.	Out of scope for FIPS 201. Requirements for the subject field of certificates are specified in Section 3.1.1 of [COMMON].
DAON-3	Daon	CT	T	42	1293	4.2.2	Although the details of the secure messaging implementation are to be contained in 800-73, it would be good to allude to whether or not mutual authentication will be optional, mandatory, or excluded. (Preference is that it not be excluded.)	Add a sentence regarding use of mutual authentication within secure messaging.	Declined. This will be specified in the next revision of SP 800-73, and the final decision on this issue will not be made until after at least one public-comment period on that document.
DAON-4	Daon	CT	G	42	1298	4.2.2	The introduction of the virtual contact interface is appreciated. It is certainly a step in the right direction.	None.	Noted and thank you.
DAON-5	Daon	CT	T	45	1421	4.2.3.3	Use of the PIN to access the biometrics (on either the contact or contactless side) still does not address the operational issues associated with PIN entry.	Reconsider PIN entry requirement (and security features that may allow for its elimination).	Noted. Biometrics is released for off-card matching after the cardholder consent. The optional OCC does not require PIN and can be alternative to off-card matching.
DAON-6	Daon	CT	T/E	52	1611	6.1	Although OMB-04-04 defines the 4 levels, it is SP 800-63 that specifies the identity proofing requirements for each of these levels. Therefore, if the PIV card meets or exceeds level 4 requirements, is it not the 800-63 requirements that are being met?	Suggest referencing [SP 800-63] here.	Declined. OMB M-04-04 is the more appropriate reference here since it is a reference to the level of assurance and not the technical requirements for meeting that level of assurance.
DAON-7	Daon	CT	E	53	1654	6.2.1	Call me insecure, but do we need to start this list with a negative characteristic?	Move 1st bullet (line 1655) to after the current 2nd or 3rd bullets.	Accept.
DAON-8	Daon	CT	E	55	1684	6.2.2	Most of the method descriptions include a bullet list of steps whereas the OCC-AUTH describes them in prose. For consistency and clarity, these would be best reformatted into a bullet list.	Bulletize the steps for OCC-AUTH as done with other methods	Declined. The OCC-AUTH authentication mechanism is being described with less detail since the technical details of the implementation, which will appear in the next revision of SP 800-73, have not yet been finalized.
DAON-9	Daon	CT	T	60	1857	6.3.2	Table 6-3. For physical access, there are provisions to elevate assurance levels based on combinations of methods; however, this is not supported for logical access, although this same approach is taken in SP 800-63. For example, the combination of BIO and CAK (which inherently also include PIN) might be considered Very High Confidence. Additionally, use of the PIV card methods shown at levels 2 & 3 may be combined with other non-PIV factors (e.g., OOB OTP) to raise the level.	If not addressed in this version, consider including combination of methods in the future (or in a separate SP).	Declined. FIPS 201 does not address either combinations of methods or authentication methods that do not involve use of the PIV Card (e.g., OOB OTP).

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS HQ-1	DHS IMD	Siegfred Young	T	42	1338	4.4.1	The standard must ensure that chain of trust information is stored or communicated to relying parties in a secure, trustworthy, interpretable and tamper evident manner. The standard and planned guidance (800-156?) should provide clarification to include: • Method for ensuring message integrity and trustworthiness (e.g. via digitally signatures) • Graduated criteria to facilitate interpretation (high, moderate and low chain of trust and corresponding applicability) • Communication methods and data formats should be consistent with existing standards to facilitate interoperability (e.g. NIEM and BAE)		Noted and to be addressed in SP 800-156.
DHS HQ-2	DHS IMD	Siegfred Young	T	22	916	4.1.4	Provisions and standards should be defined for asserting general government roles to facilitate usability of the card for mission purposes. For example, a standard FERO indicator is planned for the revised standard. A similar approach should be implemented for other general roles such as Law Enforcement Officer; this ensures consistency, usability and interoperability. Additionally, the standard should require that asserted information on the card can be electronically verified; for example printed FERO indicator should also be electronically verifiable via data encoded within the printed area buffer.		Out of scope. A comprehensive, interoperable, and consensus based list of general government roles has not been provided for inclusion in FIPS 201-2. Moreover, zones are defined in FIPS 201-2 for agency specific text where they can print such information. Declined as per discussion with FEMA. Note, should an electronic verifiable FERO indicator be needed in the future, it can be addressed in SP 800-73.
DHS HQ-3	DHS IMD	Siegfred Young	T	1	230	1.2	Scope - Consistency of printed and encoded information on the PIVcard In many cases there are multiple locations on the PIV card which represent the same data; the guidance within FIPS 201 and relevant standards must ensure that data encoded or printed on the card is consistent for interoperability, security and usability purposes. For example, person type is represented in multiple containers on the card including: • printed topology, • printed area buffer, and • FASC-N POA (Person Organization Affiliation). Currently the guidance across the relevant standards, specifically FIPS 201, 800-104 and 800-73-3 does not ensure that the data presented in these elements is consistent, when asserted/printed/encoded.		Noted. As per SP 800-73, the mandatory printed information on the card is duplicated in the printed information buffer (PIB) and a consistency check will be done with the revision of SP 800-73. Note that SP 800-104 will be withdrawn with the release of FIPS 201-2.
DHS HQ-4	DHS IMD	Robbie Reid	G	8	533	2.7	Does this section apply to foreign nationals working within the United States for the Federal Government and contractors, and if so, does the Agency's process need to be approved by the U.S. Department of State's Bureau of Diplomatic Security? Finally, is there additional governance outside of FIPS 201-2, relating foreign nationals, to assist in the development of procedures to ensure interoperability across the Federal government?		Section 2.7 does apply to foreign nationals working within the United Sates. However, the final paragraph, which indicates a need for approval by the U.S. Department of State's Bureau of Diplomatic Security, only applies to processes involving "citizens of foreign countries who are working for the Federal government overseas," not to those working within the United States.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS TWIC-1	DHS TWIC	Gerry TWIC SME	G		N/A		FIPS 201-2 relies on SP800-73, SP800-76 and SP800-78 to provide technical details on new functionality such as on-card biometrics comparison (OCC) and the virtual contact interface (VCI). FIPS 201-2 cannot become effective before SP800-73, SP800-76 and possibly SP800-78 are updated and released. Further, NPIVP cannot validate product compliance with each SP before SP800-85 is released and the test tools developed; traditionally a long delay once a version of FIPS 201 is released. To minimize the delay after FIPS 201-2 publication and before the first compliant product can be tested and eligible for listing on the GSA APL, might notall these Special Publications be released as draft for public comments simultaneously with FIPS 201-2 (as has been done for SP800-76)? Could the NPIVP validation tool be developedin parallel withthe update of SP800-85?	COMMENT: Immediately release for public comments all the FIPS 201-2 impacted Special Publications (SP) that would be needed to develop and validate compliance with FIPS 201-2 to shorten the development cycle for manufacturers.	Declined. Draft versions of SP 800-73-4, SP 800-78-4, SP 800-156, and SP 800-157 will be released for public comment as soon as they are ready. As noted in the "Effective Date" section, new features of the standard will not become effective until the related special publications have been released. However, since all mandatory-to-implement features of FIPS 201-2 are already fully specified, agencies can be compliant with FIPS 201-2 even if the special publications specifying some of the optional-to-implement features have not yet been released.
DHS TWIC-2	DHS TWIC	Gerry TWIC SME	T	2		1.3.2	A non-backward compatible change is a change or modification to an existing feature such that the modified feature cannot be used with existing systems. For example, changing the format of the biometric data would not be compatible with the existing system, because a biometric authentication attempt with the modified format would fail. Similarly, changing the PIV Card Application IDentifier (AID) would introduce a non-backward compatible change. As a result, all systems interacting with the PIV Card would need to be changed to accept the new PIV AID.	COMMENT: Relying system components deployed prior to FIPS 201-2 would be required to recognize multiple AIDs as no agency will re-issue all cards in the field immediately after FIPS 201-2 adoption. Further, if some current implementations do NOT use a partial AID SELECT command the specification might include an additional byte in the PIX portion of the PIV AID indicating the new version number and hence allowing current systems to properly SELECT the PIV application without modification.	Noted. Section 1.3 specifies general principles for change management. No decision has been made to change the PIV Card Application IDentifier (AID).
DHS TWIC-3	DHS TWIC	Gerry TWIC SME	T	2		1.3.2	For example, new mandatory features introduced in a revision of this Standard may necessitate a new PIV Card Application version number so that systems can quickly discover the new mandatory features.	PROPOSED ADDITION: The Response to SELECT defined in SP 800-73 shall be modified to conform to ISO/IEC 7816-4:2005 Application template syntax. The current Response to SELECT is not conformant to ISO/IEC 7816-4:2005.	Out of Scope for FIPS 201. Noted for SP 800-73
DHS TWIC-4	DHS TWIC	Gerry TWIC SME	E	57		6.2.5	the word If is spelled as aIF	PROPOSED CHANGE: change "aIf" to "if"	Noted. This comment is referring to the first draft of FIPS 201-2. The error has already been corrected in Revised Draft FIPS 201-2.
DHS TWIC-5	DHS TWIC	Gerry TWIC SME	T	24		4.1.4.1	"The font size 7 point allows space for 3 lines and shall only be used if the full name is greater than 45 characters. " Actually what is important is not as much the number of characters than the number of "W" vs "I" type of letters present in the name.	PROPOSED CHANGE: "The font size 7 point allows space for 3 lines and shall only be used if the name does not fit on two lines with font 8."	Resolved by changing the sentence to: The font size 7 point allows space for 3 lines and shall only be used if the name does not fit on two lines with font size 8 point.
DHS TWIC-6	DHS TWIC	Gerry TWIC SME	T	24		4.1.4.1	What should be the criteria used by the printer to decide whether to print SMITH-JONES, SUSIE MARGARET versus SMITH-JONES, SUSIE MA> RGARET ? One way to solve this issue is to ask the card holder to define during enrollment what part of the name should be on each 3 lines and have enrollment software compute the actual space needed depending on the letters used to validate the card holder choice.	PROPOSED ADDITON: Add a sentence that states the card holder name is to be printed as jointly determined by the card holder and the PIV card issuer at time of biographical data capture during enrollment.	Declined. The issuer may determine the criteria for deciding how to split a name across lines.
DHS TWIC-7	DHS TWIC	Gerry TWIC SME	T	26		4.1.4.3	Could you please define more precisely the Tactile markers to be used in zones 21F and 22F? Are there any standards to reference for purposes of compliance? What validation testing would ensure the effectiveness of these markers?	PROPOSED CHANGE: Provide technical specifications or reference to a standard to define the tactile markers that are acceptable for zones 21F and 22F and validation procedure for same.	Declined. Zones 21F and 22F are intended to provide optional placement of orientation markers and possible response to meeting 508 compliance. Federal agencies and departments are advised to coordinate implementation of the requirements with card manufacturers/vendors, and should determine the appropriate specification.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS TWIC-8	DHS TWIC	Gerry TWIC SME	T	26		4.1.4.3	Tactile markers are allows the card to exceed the maximum thichkness per ISO/IEC 7810. "shall not exceed 54 mil". How does the Standard address card readers that capture the entire card?	PROPOSED ADDITION: Add cautionary language that card capture style card reader designs will not be able to accept such a card in contact mode. COMMENT: ISO/IEC 7810 specifies a maximum thickness for a smart card. Adding tactile markers presents serious issues for card printers and lamination sub-systems. Use of tactile markers must be detailed in terms of when such markers would be introduced in the personalization process.	Declined. As specified in lines 1155-1158 and 1161-1163, the tactile markers on PIV cards have to be coordinated between agencies and manufacturers to ensure full compliance with standards relevant to FIPS 201 such as ISO/IEC 7810.
DHS TWIC-9	DHS TWIC	Gerry TWIC SME		36		4.1.6.1	The language at line 1132 reads "Two biometric fingerprints or if fingerprints are not collectible, two iris images." Since this section details MANDATORY data elements it implies iris is promoted to MANDATORY under this condition. As very few card holders would trigger this condition it seems a very burdensome requirement to have iris enrollment and data elements for only an exception case.	PROPOSED CHANGE: + Two biometric fingerprints or if fingerprints are not collectible, the facial image shall be placed on the card. RATIONALE: As facial image capture is mandatory would it not make more sense to require placement of the facial image on the card if no fingerprints cannot be enrolled? This methodology would also work for applicants with eye trauma (such as blindness).	Noted. This comment is referring to the first draft of FIPS 201-2. The requirements were changed in Revised Draft FIPS 201-2.
DHS TWIC-10				40		4.3	PIV Authentication (private) Key. "This key shall be generated on the PIV Card. " This statement is overly restrictive as a PIV Card Issuance system may elect, for large populations of PIV cards, to import this key using a secure personalization facility.	PROPOSED CHANGE: This key may be generated on the PIV Card or imported to the card. (Same language as already exists for the Key Management (private) Key).	Declined. Off-card generation of key management keys is generally considered to be a best practice in order to support key recovery. For other types of keys, however, on-card generation of keys is generally considered to be a best practice. If FIPS 201 permitted the PIV Authentication or digital signature key to be generated off-card, this could reduce the perceived level of assurance that can be provided by these keys.
DHS TWIC-11				41		4.3	Asymmetric Card Authentication (private) Key. "This key shall be generated on the PIV Card." This statement is overly restrictive as a PIV Card Issuance system may elect, for large populations of PIV cards, to import this key using a secure personalization facility.	PROPOSED CHANGE: This key may be generated on the PIV Card or imported to the card. (Same language as already exists for the Key Management (private) Key).	Resolved by changing the sentence beginning on Line 1349 from: The asymmetric Card Authentication key shall be generated on the PIV Card. To: The asymmetric Card Authentication key may be generated on the PIV Card or imported to the card. As the PKI-CAK authentication mechanism only provides SOME confidence in the asserted identity's validity (since the private key may be used without cardholder activation), permitting off-card generation of the key pair should not reduce the perceived level of assurance provided by the associated authentication mechanism.
DHS TWIC-12				41		4.3	Symmetric Card Authentication Key. "The symmetric card authentication key is imported onto the card by the issuer." The current statement is not normative as it does not include a shall. Further, this statement is overly restrictive as a PIV Card Issuance system may elect, for large populations of PIV cards, to generate this key on card using a seed value, a cryptograhpic algorithm and static data.	PROPOSED CHANGE: This key may be generated on the PIV Card or imported to the card. (Same language as already exists for the Key Management (private) Key).	Resolved by changing the two sentences beginning on Line 1362 from: The symmetric Card Authentication key is imported onto the card by the issuer. The PIV Card shall not permit exportation of this key. To: The symmetric Card Authentication key may be imported onto the card by the issuer or be generated on the card.
DHS TWIC-13				41		4.3	Digital Signature (private) Key. "This key shall be generated on the PIV Card. " This statement is overly restrictive as a PIV Card Issuance system may elect, for large populations of PIV cards, to import this key using a secure personalization facility.	PROPOSED CHANGE: This key may be generated on the PIV Card or imported to the card. (Same language as already exists for the Key Management (private) Key).	Resolved by DHS TWIC-10

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS TWIC-14				42		4.3	(Symmetric) Card Management Key. "The symmetric card authentication key is imported onto the card by the issuer." The current statement is not normative as it does not include a shall. Further, this statement is overly restrictive as a PIV Card Issuance system may elect, for large populations of PIV cards, to generate this key on card using a seed value, a cryptograhpic algorithm and static data.	PROPOSED CHANGE: This key may be generated on the PIV Card or imported to the card. (Same language as already exists for the Key Management (private) Key). SUGGESTION: The use of a Diffie-Hellman key exchange might be employed to establish a long term symmetric key for the card.	Resolved by changing the sentence beginning on Line 1388 from: The PIV Card Application Administration Key is imported onto the card by the issuer. To: If present, the PIV Card Application Administration Key shall be imported onto the card by the issuer.
DHS TWIC-15	DHS TWIC	Gerry TWIC SME	T	42		4.3	Could a symmetric key or SEED key to create a diversified symmetric session key be used as well to establish the secure messaging like Global Platform SCP03?	PROPOSED ADDITION: The PIV Card may include a symmetric key or an asymmetric private key and corresponding public key certificate to establish symmetric session keys for use with secure messaging, SUGGESTION: A One Time Password (OTP) authentication might trigger such a diversified session key creation.	Declined. The use of symmetric keys to establish secure messaging would not be interoperable. While symmetric keys may be used to establish secure messaging to perform card management operations (e.g., post-issuance update), the method used to establish such secure messaging is outside the scope of FIPS 201-2, and so is not covered in Section 4.2.2.
DHS TWIC-16	DHS TWIC	Gerry TWIC SME	T	44		4.3	Can the PIV card managment key be used over the virtual contact?	PROPOSED CHANGE: If present, the cryptographic operations that use the PIV Card Management Key must only be accessible using the contact or virtual contact interface of the PIV Card.	Declined. The PIV Card Application Administration Key is used by the issuer, whereas the virtual contact interface is established by the cardholder.
DHS TWIC-17	DHS TWIC	Gerry TWIC SME	T	42		4.4	The language states "..if no fingerprints can be collected, two electronic iris images shall be stored on the PIV card." Since this section implies iris is promoted to MANDATORY under this condition. As very few potential card holders would trigger this condition it seems a very burdensome requirement to have iris enrollment and data elements for use only in an exception case.	PROPOSED CHANGE: if no fingerprints can be collected, the facial image shall be stored on the PIV card. RATIONALE: Preserves the current enrollment station configuration per FIPS 201-1.	Noted. This comment is referring to the first draft of FIPS 201-2. The requirements were changed in Revised Draft FIPS 201-2.
DHS TWIC-18	DHS TWIC	Gerry TWIC SME	T	42		4.4	The biometric data stored on the card may also be readable through the virtual contact interface after presentation of a valid PIN. FIPS 201-2 indicates the details of the virtual contact interface will be defined in SP 800-73. It is proposed to permit the ability to read the biometric over the virtual contact interface WITHOUT A PIN as long as a secured communciation session between the card and the reader has been established. While the next revision to SP 800-73 may or may not define a mechanism where the card can trust the reader, it is conceivable that such a mutual authentication capability could be added to SP 800-73.	PROPOSED CHANGE: "…may optionally be readable through the virtual contact interface. A PIN is not required if the communication session established between the card and the reader has been secured in a manner that is in accordance with [SP 800-73]." COMMENT: TWIC proposes the use of a new Public / Private key pair data object used to securely transmit from the reader to a PIV card a (random or pseudo-random) SEED value that is used on both sides of the smart card interface to create a set of short life session variables; specifically a symmetric encryption key, a symmetric message authentication code (MAC) key and a sequence counter. The secure session may be limited to securing card to reader data though a bi-directional secure session is strongly encouraged.	Declined. The reason for requiring the presentation of a PIN before the biometric data may be read from the card is to ensure that the reader is authorized to obtain the biometric data (i.e., the cardholder authorizes the reader to obtain the biometric data by providing the PIN). While some form of mutual authentication will be required to establish the virtual contact interface, the reader-to-card authentication will not be sufficient to establish that the cardholder has authorized the reader to access the biometric data on the card. See also DAON-5.
DHS TWIC-19	DHS TWIC	Gerry TWIC SME	T	42		4.4	On-card biometric comparison may be performed over the contact and the contactless interfaces of the PIV Card to support card activation	PROPOSED CHANGE: On-card biometric comparison may be performed independent of the communications interface in effect to support card activation.	Declined. The full sentence being quoted says "The on-card biometric comparison data may be available through the contact and the contactless interface of the PIV Card to support card activation (section 4.1.7.1) and cardholder authentication (section 6.2.5)." Privileged operations, which require card activation, may only be performed over the contact and virtual contact interfaces.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS TWIC-20	DHS TWIC	Gerry TWIC SME	T	57		6.2.5	If the fingerprints for on card comparison are the same as the fingerprints for off card comparison, getting access to the fingerprints for off card comparison is equivalent to reading the value of the PIN, as such value can be submitted later on by a malware to activate the card through OCC-AUTH. We would recommend when possible to use different fingers for on-card comparison than the ones used for off card comparison.	PROPOSED CHANGE: Two fingerprints, for on-card comparison, which are preferably not the same as the two fingerprints collected for off-card comparison.	Resolved by AMAG-5.
DHS TWIC-21	DHS TWIC	Gerry TWIC SME	E	57		6.2.5	the word If is spelled as aIF	PROPOSED CHANGE: change "aIf" to "if"	Noted. This comment is referring to the March 2011 draft of FIPS 201-2. The error has already been corrected in Revised Draft FIPS 201-2.
DHS TWIC-22	DHS TWIC	Gerry TWIC SME	T	57		6.25	Authentication Using On-Card Biometric Comparison (OCC-AUTH): The FIPS 201-2 Standard states the response includes information that allows the reader to authenticate the card. However, according to ISO/IEC 7816-4 the VERIFY command using CLA (class) byte '0x' shall not return any response data besides the two byte status word. As such, no authentication data can be returned using this form of the VERIFY command. To complicate matters, it is stated earlier in the FIPS 201-2 document that a successful OCC_AUTH can be used to activate the PIV card and therefore unlock the PIV Authentication key allowing a card holder authentication to proceed as if the PIN was verified. To achieve satisfying access conditions this funtion has to be a two step process (more than one APDU command) OR a proprietary form of the VERIFY command must be used (with CLA (class) byte of the form '8x').	PROPOSED CHANGE: rewrite this section to clearly articulate what is meant to be achieved and how it will be achieved (i.e. by a single proprietary APDU command or a sequence of ISO APDU commands).	Declined. Specific details of the implementation of on-card biometric comparison will be specified in SP 800-73-4, not in FIPS 201-2. However, it should be noted that if the VERIFY command is performed over secure messaging, which was established with card-to-reader authentication, then the status response from the VERIFY command can be authenticated, and can be used as the basis for determining whether the on-card biometric comparison was successful. Further details are provided in the initial draft of SP 800-73-4. Appendix B.1.4 of Part 1 provides additional details about the implementation of the OCC-AUTH authentication mechanism. Section 4.2 of Part 2 (and in particular Section 4.2.5) shows that when the VERIFY command is submitted over secure messaging, the two-byte status word is protected with a MAC, thus allowing the status word to be authenticated.
DHS TWIC-23	DHS TWIC	Gerry TWIC SME	T	58		6.26	A unique identifier within the data element is used as input to the authorization check to determine whether the cardholder should be granted access. Since the data element is no longer always the CHUID but could now be also from an authentication certificate, how does the reader know which data element to use?	PROPOSED CHANGE : Rewrite this section to state what elements shall be used, and in what order, as input to any (static) authorization check by an external privilege granting system to determine whether the card holder should be granted access. SUGGESTION: One elegant solution is to use one of the currently unused mode values of RFC 4122 to indicate "GUID contains a FASC-N value". This would allow PIV cards to migrate to using the GUID as the binding element without impacting current FASC-N enabled operations on the reader or relying system (e.g. PACS).	Declined. The type of unique identifier that needs to be provided by the reader will be determined by what the authorization system requires. Decline to allow creation of UUID values that are not created in conformance with RFC 4122. Current relying systems are not impacted by the requirement to include UUID values on PIV Cards, since the FASC-N continues to be a mandatory data value.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-1	DoD	Jonathan Shu	Critical (Technical)	General and pg. 42	General and 1284-1390	General and 4.2.2	While DoD understands the desire to incorporate information into FIPS-201 for future capabilities, there are significant concerns about the maturity and security of standards-based secure contactless capabilities. DoD needs to better understand the risks before signing off on the special publication(s) that prescribe communication of biometrics, personal identifiable information (PII), or people-oriented PKI transaction (i.e., authentication, digital signing, and encryption) over the contactless interface. These new desired capabilities may introduce unacceptable levels of risk/vulnerabilities and weaken the sound authentication and trust build by the use of PIVs and PKI.	DoD does not agree with expanding the authorization of exchanging PIV contact over the contactless interface unless (and before the relevant special publications are finalized) NIST agrees to: (a) conduct a security evaluation on the various methods for secure contactless communications as outlined within emerging NIST SP 800-157 and 800-73-4 (if applicable), (b) share those findings with federal agencies' PIV/PKI leads, and (c) provide a decision brief to the Federal CIO Council or Federal CIO Council's ISIMC on the findings from the security evaluations and recommendation on next steps for communicating other PIV objects over contactless interface. DoD feels these actions will allow the senior security and IT leadership of the federal government to clearly understand the risks before setting out to make these new capabilities available.	Noted. A draft version of SP 800-73-4 has been made available for public comment, and a draft version of SP 800-157 will be made available for public comment before the final version is published. In addition, support for these features is optional to implement.
DoD-2	DoD	Jonathan Shu	Critical (General)	vii	196	10. Foreword	With regard to the requirement, "To comply with FIPS201-2, all new and replacement PIV Cards shall be issued with the mandatory PIV Card features no later than 12 months after the effective date of this standard." DoD will have trouble meeting the changes in the timeframe because of resource limitations, acquisition cycles, and testing processes to ensure DoD's CAC PIV capabilities continue to operate seamlessly.	Recommend changing the requirement to: "To comply with FIPS201-2, all new and replacement PIV Cards shall be issued with the mandatory PIV Card features no later than 24 months after the effective date of this standard."	Declined. After discussions with OMB it has been determined that this requirement will remain unchanged.
DoD-3	DoD	Jonathan Shu	Critical (Technical)	6	404-407	2.4	The requirement, "If the biometric data that is collected as specified in this section and in Section 2.3 is collected on separate occasions, then a 1:1 biometric match of the applicant shall be performed at each visit against biometric data collected during a previous visit." appears to imply that if biometric data for background investigations where taken separately, then a 1:1 biometric match from the 10-print (from the background investigation) is necessary when collecting the two fingerprints during card issuance of new applicants.	Recommend changing the requirement to: "If the biometric data that is collected as specified in this section and in Section 2.3 is collected on separate occasions, then a 1:1 biometric match of the applicant shall be performed at each visit against biometric data collected during a previous visit only if the individual has been previously issued a PIV." Continuing to link the biometrics taken during the background investigations and those used in PIV issuance would require significant changes to DoD's CAC/PIV issuance systems and substantial investments to fully integrate these separate processes. DoD strongly recommends this mandated link between background investigation and issuance biometrics be severed.	Declined. As discussed with OMB and the HSPD-12 core team, extended enrollment should adhere to the same requirements as one-time collection for both 10-prints and 2-prints (for on-card fingerprints) in order to maintain the control objective -- regardless of the method used. (The person who's been checked is the person receiving the card). Extended enrollment can be achieved if the 10 prints are matched with the fingerprints to be stored on-card. See also Cert-88, WM-24, and DOJ-12 in the disposition of comments for March 2011 Draft FIPS 201-2.
DoD-4	DoD	Jonathan Shu	Editorial	6	408	2.4	The statement, "The choice of which two fingers is important and may vary between persons." has dubious value.	Recommend deleting the sentence.	Declined. This sentence is needed as an explanation for the following sentence: "The recommended selection and order is specified in [SP 800-76]."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-5	DoD	Jonathan Shu	Critical (Technical)	7	Footnote	2.6	Footnote #3 states the chain of trust must include biometric data used in the background investigation process. This should not be the case because background investigations and cards issuance/maintenance are separate and unrelated processes.	Recommend deleting footnote because continuing to link the biometric data taken during the background investigations with those used in PIV issuance would require significant changes to DoD's CAC/PIV issuance systems and substantial investment to fully integrate these separate processes. DoD strongly recommends this mandated link between background and issuance biometrics be severed.	Resolved by DoD-3.
DoD-6	DoD	Jonathan Shu	Critical (Technical)	41098	Line 435, Reference 3. Also see lines 404 - 406, 464 - 465, & 474- 475.	3	While Section 2.6 (line 431) identifies the chain of trust as optional, it seems to require biometric matches of fingerprints taken from the 10-print background investigation process with those within PIV issuances.	Continuing to link the biometrics taken during the background investigations and those used in PIV issuance would require significant changes to DoD's CAC/PIV issuance systems and substantial investments to fully integrate these separate processes. DoD strongly recommends any link between background investigation and issuance biometrics be severed.	Resolved by DoD-3.
DoD-7	DoD	Jonathan Shu	Critical (Technical)	8	461-465	2.6	The "extended enrollment" example continues to connect biometrics collected during the background investigation with those within the chain of trust and PIV issuance process.	Strongly recommend including a different example that more accurately reflects the separation of biometrics for background investigations from those used in the PIV issuance process.	Declined. Other examples are already given in this section. Extended enrollment example should not be removed since it is a valid use case for Chain-of-trust. See also DoD-3.
DoD-8	DoD	Jonathan Shu	General	Revised Page 9	Line 485 - 487. Also see lines 548 - 552	3	Current OMB guidance allows an interim credentialing determination to be issued based upon initiation of a NACI or other equal or greater national security investigation and favorable notification of results from the FBI National Criminal History Check.	Recommend change and clarification in the language to allow interim PIV issuance following initiation of a NACI (or equal or greater suitability or national security investigation) and favorable notification of results of the FBI National Criminal History Check.	Declined. The text in Revised Draft FIPS 201-2 was written in coordination with OMB and OPM to align with M-05-24, which says in part: Initiate the National Agency Check with Written Inquiries (NACI) or other suitability or national security investigation prior to credential issuance. Before issuing the credential, agencies should receive notification of results of the National Agency Checks. If you do not receive the results in 5 days, the identity credential can be issued based on the FBI National Criminal History Check (fingerprint check).
DoD-9	DoD	Jonathan Shu	General	9-10	489	2.7	The text has been updated in FIPS-201 to specify documents rather than referencing the I-9 form.	Recommend updating Federal Bridge CP to match the text in FIPS-201 regarding acceptable forms of identity documentation for the issuance of PIV-I cards. It is our understanding that the intent is for PIV-I requirements to mirror PIV whenever possible.	Out of Scope. The Federal Bridge CP is maintained by the Federal PKI Policy Authority.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-10	DoD	Jonathan Shu	Critical (General)	10	530-532 and 541-542	2.7 and 2.8	The section states, "The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head or deputy secretary (or equivalent) of the federal department or agency." The requirement for "head or deputy secretary" approval does not appear to be necessary and contradicts those roles outlined within NIST SP 800-79-1. NIST SP 800-79-1 and other C&A type processes within the Federal government allowed agencies (if desired) to delegate approval to areas of their organization that are much closer to the program managers and policy leads responsible for the IT infrastructure being operated (i.e., PIV issuance systems).	Strongly recommend deleting this sentence to allow agencies to move the approval closer to the individuals that manage and oversee the issuance systems.	Declined. The quoted text specifies requirements for approval of the identity proofing and registration process. It is not imposing a requirement on who may be the approving authority for the PIV issuance systems.
DoD-11	DoD	Jonathan Shu	Critical (Technical)	11	557-560	2.8	The requirement, "Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the applicant against biometrics available on the PIV Card." is too specific and restricts PIV issuers from implementing other security techniques to ensure the individual who receives the card is the individual that provided the biometric data. Perceived security enhancements do not appear to warrant the cost (time in issuance process and resources) to re-engineer issuance processes or actually improve security. A more generic requirement should be outlined.	Recommend the requirement be changed to: "Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the applicant against available biometrics (either stored within the issuance infrastructure or on the PIV Card)." This will provide flexibility for PIV issuers. It is unclear why the biometric data placed on the card must be matched before completing issuance with the individual when, for DoD, the issuance process includes identity proofing. This is a manned process overseen by a trusted operator and is conducted on restricted access workstations/systems.	Resolved by changing sentence to read: Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the applicant against biometrics available on the PIV Card or in the chain-of-trust. The goal of the 1:1 biometric match is to ensure that the person receiving the card is the actual cardholder
DoD-12	DoD	Jonathan Shu	Technical	12	581	2.82	A maximum time for a lapse period should be specified when an individual ceases to be a federal employee or contractor. The timeframe should align with federal personnel security re-investigation requirements.	Recommend the lapse in an individual's status as a federal employee or contractor coincide with DoD credentialing guidance. "No break in service greater than 24 months and the individual has no actionable information since the date of the last completed investigation."	Resolved by OPM-28.
DoD-13	DoD	Jonathan Shu	Editorial	14	642	2.9.1	It would be helpful to clarify the revocation requirements for renewal and reissuance. Recommend changing Section 2.9.1 to reflect the proposal expressed at the FIPS 201 Workshop.	Recommend changing to "When a PIV Card is reissued or renewed, it is mandatory to revoke certificates only if the PIV card is not returned to the issuer, is lost or stolen, or if the PIV card or keys are compromised or suspected of compromise. Departments and agencies may enforce a more stringent certificate revocation policy for their PIV card holders."	Resolved by AMAG-11. Section 4.9.3 of [COMMON] already notes that revocation of certificates is recommended even if cases in which it is not mandatory.
DoD-14	DoD	Jonathan Shu	General	12, 13-14	653	2.8.2, 2.9.2	The text here allows for reissuing a card after a compromise through collecting new biometric data and comparing it against an existing biometric chain of trust. However, [COMMON] requires that a lost, stolen, or otherwise compromised credential have all certificates revoked. Additionally, all steps performed at initial authentication must be repeated to issue a new certificate after revocation. Reissuance should require the initial identity proofing steps in the event of compromise. Since a lost or stolen card is assumed to be compromised, these cases also require the initial identity proofing steps.	Recommend change the last sentence of the first paragraph as follows: "The entire identity proofing, registration, and issuance process, as described in Sections 2.7 and 2.8, shall be repeated for cards that have been compromised, lost, or stolen. For cards which have been damaged, the entire identity proofing, registration, and issuance process shall be repeated if the issuer does not maintain a chain-of-trust record for the cardholder or if the cardholder did not apply for reissuance before the original PIV Card expired."	Declined. The identity proofing and registration process in FIPS 201-2 includes steps that are not required by [COMMON] for the issuance of certificates (e.g., the collection of biometric data to be stored on the card). So, even if the initial registration process as specified in [COMMON] needs to be repeated in the case of compromised, lost, or stolen cards, there are still benefits to be gained in terms of efficiency in not requiring the entire FIPS 201-2 identity proofing and registration process to be repeated. Furthermore, [COMMON] could be changed to streamline the certificate issuance process in cases in which the applicant's identity can be verified by a 1:1 biometric match against data stored in the issuer's records.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-15	DoD	Jonathan Shu	Editorial	14	674-677	2.9.2	The wording for this section is unclear and should be more straight forward.	Recommend restating that "All certificates associated with private keys that are stored on the card shall be revoked."	Declined. Some protocols that are under consideration for the establishment of secure messaging make use of card verifiable certificates (CVC), which cannot be revoked. If such a protocol were to be selected then there would be a private key on the PIV Card whose associated certificate could not be revoked.
DoD-16	DoD	Jonathan Shu	Critical (Technical)	15	714-716	2.9.4	The bullet states, "When PIN reset is performed in-person at the issuer's facility, the issuer shall ensure that the cardholder's biometric data matches that stored on the reset PIV Card, through an on-card or off-card 1:1 biometric match, before providing the reset PIV card back to the cardholder." The requirement is too specific and restricts PIV issuers from implementing other security techniques to ensure the individual seeking a reset PIN is the individual to whom the card was issued.	Recommend changing to "When PIN reset is performed in-person at the issuer's facility, the issuer shall ensure that the cardholder's biometric data matches available biometric data (either stored within the issuance infrastructure or on the PIV Card), through an on-card or an off-card 1:1 biometric match, before providing the reset PIV Card back to the cardholder" This will provide flexibility for PIV issuers while maintaining the same level of assurance that the individual is the original cardholder.	Resolved by changing the sentence to read: When PIN reset is performed in-person at the issuer's facility, before providing the reset PIV Card back to the cardholder, the issuer shall perform a 1:1 biometric match to ensure that the cardholder's biometric matches either the stored biometric on the PIV Card or biometric data stored in the chain-of-trust.
DoD-17	DoD	Jonathan Shu	Critical (Technical)	15	721-733	2.9.4	Performing biometric collection from an unattended kiosk requires additional security controls to ensure that the biometric was actually collected at the kiosk and that the kiosk has not been tampered with.	Recommend requiring additional security controls on the kiosk, including verifying the kiosk's own identity prior to performing the reset and ensuring that the kiosk has not been tampered with (e.g., through physical security controls on the location of the kiosk and through periodic checks of the kiosk itself).	Out of scope. There are many agency-specific variables to consider, which makes specific security measures as suggested by this comment too restrictive or unnecessary. It is more appropriate for each agency to apply SP 800-53 controls rather than to specify it in FIPS 201-2. For example, the security controls of SP 800-53 may be quite different for a kiosk in a secured area as opposed to at a kiosk in a lobby.
DoD-18	DoD	Jonathan Shu	Critical (Technical)	15	725-733	2.9.4	Allowing the end user to use a general computing platform to collect and submit biometric data creates a significant new vulnerability. Someone could find a card and represent themselves remotely as the legitimate card holder by submitting the card holder's biometric rather than their own to get the activation data reset. Having a requirement that the operator authenticate the owner of the PIV Card through an out-of-band authentication procedure does not sufficiently offset this vulnerability.	Recommend removing text allowing unattended biometric collection as part of activation data reset.	Declined. The remote reset procedure does not involve "submitting" or "collecting" biometric data. It involves performing on-card biometric comparison. An attacker who is capable of successfully performing the on-card biometric comparison will already have the ability to activate the card and perform operations using all of the private keys on the card. Furthermore, the ability to perform remote PIN resets is a highly sought after capability. No alternative procedure for enabling remote PIN resets has been proposed.
DoD-19	DoD	Jonathan Shu	Editorial	16	749	2.9.5	How does termination differ from what happens as part of reissuance? One could read termination as what happens when a card is terminated and no new one is issued, but it would be nice to see that explicitly spelled out.	Recommend adding a definition or point of clarification for termination. This will provide a distinction between termination and the termination portion of reissuance process (as described in section 2.9.2).	Resolved by adding the following sentence to the beginning of Section 2.9.5 (now Section 2.9.4): A PIV card is terminated when the department or agency that issued the card determines that the cardholder is no longer eligible to have a PIV Card.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-20	DoD	Jonathan Shu	Substantive (Technical)	16	765	2.9.5	It is unclear why PIV Auth and aCAK must be revoked in benign circumstances, while revocation is optional for digital signature and key management certificates.	Recommend eliminating the requirement to revoke PIV Auth and aCAK certificates in benign circumstances.	Resolved by changing: The CA shall be informed and the certificates corresponding to PIV Authentication key and the asymmetric Card Authentication key on the PIV Card shall be revoked. If the PIV Card cannot be collected, the certificates corresponding to the digital signature and key management keys shall also be revoked, if present. If the PIV Card is collected and destroyed, then revocation of the certificates corresponding to the digital signature and key management keys is optional. To: If the PIV Card cannot be collected and destroyed, the CA shall be informed and the certificates corresponding to the PIV Authentication key and the asymmetric Card Authentication key on the PIV Card shall be revoked. The certificates corresponding to the digital signature and key management keys shall also be revoked, if present.
DoD-21	DoD	Jonathan Shu	Substantive (Technical)	16	768-771	2.95	This section states, "If the card cannot be collected, normal termination procedures shall be completed within 18 hours of notification." As part of normal termination procedures in lines 761 through 765, revocation of certificates is addressed. The common policy says that revocation should occur as quickly as practical upon receipt of a proper revocation request with references to when the next CRL is published. This differs from the 18 hour specification in FIPS 201-2.	Recommend that FIPS 201-2 refer to timeframes specified in the common policy for revocation of certificates associated with termination of the PIV card and not include revocation of certificates in the 18 hour timeframe.	Declined. The Common Policy specifies requirements for how quickly a CA needs to process a revocation request, but does not impose specific requirements for how quickly a revocation request must be submitted. This is addressed in FIPS 201-2 by including the informing of the CA as part of the normal termination procedures.
DoD-22	DoD	Jonathan Shu	Substantive (Technical)	17	775-776	2.10	This section states, "When a cardholder's PIV Card is terminated as specified in Section 2.9.5, any PIV derived credentials issued to the cardholder shall also be terminated." It is DoD's belief that the derived credential's fate needs to be tied to the certificate from which it was derived, not just the card.	Recommend to rephrase this to require termination of the derived credential when the certificate (or other PIV data) from which it was derived is terminated. (e.g., via revocation or expiration)	Declined. While individual issuers of derived credentials may choose to implement such a policy, it would be an unnecessary burden to impose it on all issuers.
DoD-23	DoD	Jonathan Shu	Substantive (Technical)	17	776	2.10	The derived credential concept is useful, and DoD awaits the publication of SP 800-157. There will be a need for improved record keeping so it is possible to identify derived credentials when revocation is necessary.	Recommend adding: "Note that improved record keeping will be required so that it is possible to identify derived credentials when revocation is necessary."	Out-of-Scope. Information such as this will be specified in SP 800-157.
DoD-24	DoD	Jonathan Shu	Substantive (Technical)	29	1094-1096	4.1.4.1	The section outlines a requirement for government PIVs to contain a circle "W" within the blank white space to represent white. This requirement is over prescriptive and can easily be accommodated by a lack of circle letter in the space to denote the color white and government employees.	Recommend deleting the requirement to include a circled "W" for PIVs issues to government employees that do not contain a bar stripe.	Declined. For consistent treatment of the color bar, the circled 'W' is required.
DoD-25	DoD	Jonathan Shu	Substantive (Technical)	41	1247	4.2	DoD would prefer to have the flexibility to combine the PIV Auth and digital signature keys/certificates to reduce the number of certificates and resulting CRL size, as well as provide potential usability advantages. This recommendation would need to be implemented in concert with the recommendation in 4.2.2 to tie explicit user action to the application rather than the key.	Recommend moving asymmetric key pair and certificate for digital signature from the mandatory to the optional section, with the proviso that if there is an email account either the PIV Auth certificate must be used for digital signature or a separate digital signature key pair/certificate must be on the card.	Resolved by DoD-30.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-26	DoD	Jonathan Shu	Critical (Technical)	42	1298-1303	4.2.2	The term "Virtual Contact Interface" lacks scope definition. It is confusing throughout the document when the VCI means contact or contactless. Furthermore, the use of "contact" in the name makes it confusing when it is contactless.	Strongly recommend replacing the term "Virtual Contact Interface" with "Secure Contactless Interface" to more accurately reflect the activity and resolve any confliction/confusion.	Declined. Just as a virtual private network (VPN) is operated over a public network, but offers the properties of a private network, the virtual contact interface is operated over a contactless interface but offers the properties of a contact interface. The term "Secure Contactless Interface" would be more confusing since it could be confused as applying to all uses of secure messaging over the contactless interface.
DoD-27	DoD	Jonathan Shu	Technical	0	0	0	Throughout the document, there are places where the term "PIV Card" is used and should be change to "PIV Card Application". (i.e., Line 395: sec 2.4 "Biometric Data Collection for PIV Card..." should be changed to "....PIV Card Application," or line 413: "...stored on the PIV Card" should be changed to "stored on the PIV Card Application")	Strongly recommend using the appropriate term when referring to the PIV Card Application.	Resolved by updating the definition of PIV Card as follows: "A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable)."
DoD-28	DoD	Jonathan Shu	Technical	43	1319	4.2.2	"Optionally, up to twenty retired key management keys may also be stored on the PIV Card." Why was the number twenty picked? This seems arbitrary without additional context. That may be on the high side of what card storage space and reasonable performance support today, but larger numbers may become feasible as technology advances. If the number is only limited by the technology, it doesn't seem like we should specify it in policy.	Recommend adding context as to why twenty is the magic number, or make the allowance generic. Recommend rewriting as: "Optionally, retired key management keys may also be stored on the PIV Card."	Declined. SP 800-73 specifies that the PIV Card Application may store up to 20 retired key management keys. This number was chosen since each card application is limited to 32 key references, and several key references were already assigned for other purposes. It would be inappropriate, however, for FIPS 201-2 to include a rationale for every technical decision made in developing the Standard.
DoD-29	DoD	Jonathan Shu	Substantive (Technical)	43	1349	4.2.2	The Asymmetric Card Authentication Key provides the capability to sign an arbitrary value without requiring user activation. An attacker could potentially forge an email message, calculate the message digest, and have the aCAK sign the digest. Some protections exist (e.g., a critical EKU and absence of other allowed EKUs), but since this document requires the CAK, DoD feels the FIPS 201 does not prescribe enough protection against the ability to exploit due to the lack of PIN entry.	In recognition of occasional poor public key enabling by Relying Party, DoD recommends an additional protection whereby the card "prepends a salt" to the challenge to thwart such attacks. DoD will reiterate these concerns during the revisions of NIST SP 800-73-3.	Declined. This would be a non-backward compatible change that would break relying party applications that have been developed to use the CAK, and current PIV Cards already implement the CAK, but without the proposed feature. In addition to the fact that the critical extended key usage should prevent relying parties from inappropriately accepting data signed with the CAK, the profile for the Card Authentication certificate prohibits the inclusion of any identifying information in the certificate other than the FASC-N and UUID from the PIV Card. Thus, most applications/users would be unable to tie a signature created using the CAK to the holder of the card on which the key resides.
DoD-30	DoD	Jonathan Shu	Technical	44	1370	4.2.2	We believe the requirement for explicit user action should be tied to the application rather than the key on the card. The card cannot know whether a PIN is being provided by middleware or the actual user. Furthermore, placing the responsibility on the application would provide flexibility (e.g., a pop-up window that says "you are about to sign" or other). It would also permit the same certificate to be used for signing and authentication.	Recommend rewriting as: "Digital signature operations may not be performed by an application without explicit user action."	Declined. As described in NISTIR 7863, Cardholder Authentication for the PIV Digital Signature Key, the PIN ALWAYS requirement for the digital signature key is needed, in conjunction with the design of the application and/or middleware, to ensure that the explicit user action requirement for digital signature operations is met. For usability reasons a PIN ALWAYS requirement cannot be imposed on the PIV Authentication key.
DoD-31	DoD	Jonathan Shu	Technical	45	1413-1420	4.2.3.2	The Federal PKI CPWG didn't take action on the OID for Content Signing because FIPS-201 didn't allow it. Now the change to FIPS-201 doesn't allow the content signing OID because the FPKI CPWG didn't define it. Given that PIV-I has a content signing OID, it may make sense to have a content signing OID for PIV, as well.	Recommend replacing the beginning of the fourth paragraph of section 4.2.3.2 with the following text: "The public key required to verify the digital signature shall be contained in a content signing certificate which shall be issued in conformance with [COMMON]. If the signature on the biometric..."	Resolved by FPKI-3.
DoD-32	DoD	Jonathan Shu	Editorial	46	1433-1434	4.2.4	Identifiers are used for authentication, not authorization.	Recommend deleting: "and authorization."	Declined. Once the cardholder has been authenticated, it is an identifier associated with the cardholder that is used to make the authorization decision.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-33	DoD	Jonathan Shu	Technical	46	1458-1459	4.3.1	"The PIV Card shall include mechanisms to block activation of the card after a number of consecutive failed activation attempts." Not specifying an upper limit takes the teeth out of this requirement.	Recommend to specify a max number of consecutive failed PIN entries and biometric match-on-card attempts after which the card must be locked or outline the specific probability a card must protect against brute force or replay attacks. DoD will also provide this comment to the revision of NIST SP 800-73-3 and 800-76-2.	Out of Scope. The activation mechanism needs to satisfy the requirements of FIPS 140 in this area. This will be specified (if needed) in the associated Special Publication.
DoD-34	DoD	Jonathan Shu	Critical (Technical)	48	1503-1504	4.4.4	The last sentence states: "If the input device is not integrated with the PIV Card reader, the OCC data or the PIN shall be transmitted securely and directly to the PIV Card for card activation." This contradicts earlier requirements within this section for readers that are connected to devices for logical access. It appears to create a requirement for PIN authentication to a non-PIN pad reader through an encrypted tunnel. Most readers within DoD that support logical access are "pass through" devices that do not contain an integrated PIN pad or support encryption. This statement would require DoD to upgrade most existing readers to support tunnel encryption or integrated PIN pads. This would be a costly endeavor.	Recommend deleting this sentence.	Declined. See Cert-98 and ES-19 in the disposition of comments for March 2011 Draft FIPS 201-2.
DoD-35	DoD	Jonathan Shu	Editorial	49	1514	5.1	The following sentence appears to preclude participation through the Federal Bridge: "The CA that issues certificates to support PIV Card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI."	Recommend changing to: "A CA that issues certificates to support PIV Card authentication shall be in the Federal Common Root Hierarchy or cross-certified with the Federal Common Root."	Declined. The proposed change is unnecessary since Section 5.4 does not list Section 5.1 as a section that applies to legacy PKIs, and the quoted sentence is accurate for CAs that are not part of a legacy PKI.
DoD-36	DoD	Jonathan Shu	Technical	49	1521-1526	5.2	The Federal PKI is currently discussing possible changes to the overall architecture to streamline operations. Overly constraining the architecture and PKI requirements in FIPS-201 prevents the Federal PKI from implementing changes. Specific requirements for PKI should be addressed in [COMMON] rather than being overly specified in FIPS-201. Current sentence states: "All certificates issued to support PIV Card authentication shall be issued under the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [COMMON]."	Recommend changing the first sentence of Section 5.2 to: "All certificates used to support PIV Card authentication shall be issued in conformance with the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON[."	Declined. See DoD-58 in the disposition of comments for March 2011 Draft FIPS 201-2.
DoD-37	DoD	Jonathan Shu	Technical	49	1532-1534	5.2.1	The Federal PKI is currently discussing possible changes to the overall architecture to streamline operations. Overly constraining the architecture and PKI requirements in FIPS-201 prevents the Federal PKI from implementing changes. Specific requirements for PKI should be addressed in [COMMON] and [PROF] rather than being overly specified in FIPS-201.	Recommend deleting "and shall specify either the id-fpki-common-hardware or id-fpki-common-High policy in the certificate policies extension."	Declined. As noted in TR-1, it has been requested that this information be included in FIPS 201-2, and these are the only two policy OIDs in [COMMON] that are appropriate for digital signature certificates given the requirement in Section 4.2.2 for the digital signature key to be generated on the card and to be non-exportable, and given the need to satisfy the cryptographic algorithm requirements specified in SP 800-78. Note, however, that Section 5.4 states that "This specification imposes no requirements on digital signature or key management certificates issued by legacy PKIs."
DoD-38	DoD	Jonathan Shu	Technical	49	1532-1536	5.2.1	The End Entity Signature Certificate Profile and the PIV Authentication Certificate Profile must be compatible to support the earlier recommendation to provide the option for the PIV Auth and digital signature certificates to be combined.	Recommend that if the End Entity Signature Certificate and PIV Authentication Certificate profiles are in any way contradictory, then NIST should create an additional profile for a combined PIV Auth and signing certificate.	Resolved by DoD-30.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-39	DoD	Jonathan Shu	Technical	50	1545-1553	5.4	The original intent of this section was to clarify that legacy Federal PKIs are required to follow the requirements in Section 5.2.1, but not necessarily have to follow the requirements in the remainder of Section 5. However, with the change that signature and encryption certificates are required, and the proposed changes to this section that make all sections relevant to legacy PKIs, the section is confusing rather than useful. Rather than being overly prescriptive in FIPS-201 regarding the implementation of Federal Agency PKIs, FIPS-201 should allow the Common Policy to address these requirements.	Recommend removing Section 5.4 from the document and update [COMMON] to specify requirements for the issuance of certificates on PIV cards. Specifically, remove the requirement specifying which OIDs certificates must assert from FIPS-201 and address it in [COMMON].	Declined. [COMMON] is maintained by the Federal PKI Policy Authority and not NIST. While NIST may propose changes to [COMMON], NIST is not in a position to dictate that [COMMON] be updated to include specific information. Removing Section 5.4 would be problematic for legacy PKIs, as there are certain requirements imposed in Section 5 from which legacy PKIs are exempted in Section 5.4.
DoD-40	DoD	Jonathan Shu	Technical	50	1549-1552	5.4	Change the following paragraph: "PIV Authentication Certificates and Card Authentication Certificates issued by legacy PKIs shall meet the requirements specified in Section 5.2.1. Departments and agencies may assert department or agency-specific policy OIDs in PIV Authentication Certificates and Card Authentication Certificates in addition to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively." During the SHA-2 transition and use of new policy OID, we have discovered that asserting policy OID from one domain removes the flexibility for both sides of cross certified domain. It is desirable to map the policies to provide requisite security and flexibility to cross-certified domains. For the policy assertions to work securely, the applications should process policies and policy mapping appropriately and not just pick the policy in the end certificate. Thus, mapping to appropriate policies (as opposed to direct assertion) will provide requisite security while maintaining flexibility.	Recommend removing Section 5.4 from the document and update [COMMON] to specify requirements for the issuance of certificates on PIV cards. Specifically, remove the requirement specifying which OIDs certificates must assert from FIPS-201 and address it in [COMMON]	Declined. See DoD-58 in the disposition of comments for March 2011 Draft FIPS 201-2. In addition, [COMMON] is maintained by the Federal PKI Policy Authority and not NIST.
DoD-41	DoD	Jonathan Shu	Editorial	50	1555	5.5	Paragraph states: "The PIV PKI repository and Online Certificate Status Protocol (OCSP) responder provides PIV Card and key status information..." What is the PIV PKI repository? Is it intended to mean something more than a certificate repository? Does it contain information about the card itself in addition to information about the certificates contained thereon?	Recommend defining the PIV PKI repository to include information on how systems and/or users would access it.	Resolved by DoD-42.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-42	DoD	Jonathan Shu	Editorial	50	1555-1557	5.5	"The PIV PKI repository and Online Certificate Status Protocol (OCSP) responder provides PIV Card and key status information across departments, agencies, and other organizations, to support high-assurance interagency PIV Card interoperation." This could be read to mean that an organization's OCSP responder must provide status for all PIV cards.	Recommend clarifying the text to make the requirement applicable only to the PKI that issued the credentials.	Resolved by changing: The PIV PKI repository and Online Certificate Status Protocol (OCSP) responder provides PIV Card and key status information across departments, agencies, and other organizations, to support high-assurance interagency PIV Card interoperation. To: CAs that issue certificates to support PIV Card authentication shall operate repositories and Online Certificate Status Protocol (OCSP) responders that provide certificate status information for the certificates they issue to support high-assurance interagency PIV Card interoperation.
DoD-43	DoD	Jonathan Shu	Editorial	50	1560-1561	5.5	It is unclear what the sentence, "The expiration date of the authentication certificates (PIV Authentication certificate and Card Authentication certificate) shall not be after the expiration date of the PIV Card." has to do with PKI Repository and OCSP Responder(s). If it does or doesn't, the requirement is already specified in [COMMON].	Recommend deleting the sentence.	Declined. This requirement does not already appear in [COMMON].
DoD-44	DoD	Jonathan Shu	Technical	50	1562	5.5	It isn't clear why the authentication certificates needs to be revoked, while the other certificates do not.	DoD would prefer flexibility for all certificates to not need to be revoked, if steps are taken to preclude further use of the certificates.	Resolved by AMAG-23.
DoD-45	DoD	Jonathan Shu	Technical	50		5.5	The Federal PKI is currently discussing possible changes to the overall architecture to streamline operations. Overly constraining the architecture and PKI requirements in FIPS-201 prevents the Federal PKI from implementing changes. Specific requirements for PKI should be addressed in [COMMON] rather than being overly specified in FIPS-201. Specific requirements for protocols used to access CRLs and Certificate Status Servers should be addressed in [COMMON] and not specified in FIPS-201.	Recommend deleting the second and third paragraphs of Section 5.5, lines 1566-1574 and address these requirements in [COMMON].	Declined. The information provided in these two paragraphs is unlikely to change in the near future, and including it in FIPS 201 provides useful information to readers.
DoD-46	DoD	Jonathan Shu	Technical	50	1571-1573	5.5	"PIV Authentication certificates and Card Authentication certificates shall contain the crlDistributionPoints and authorityInfoAccess extensions needed to locate CRLs and the authoritative OCSP responder, respectively. In addition, every CA that issues these authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues." Certificate validation, which includes a revocation check, should be performed as part of any PKI operation. Thus, revocation information (ideally via OCSP as well as CRLs) for all certificates must be available, and all certificates need to contain information regarding where to retrieve revocation information.	Recommend these details be required for all certificate and subsequently address in the certificate profile requirements in [COMMON].	Resolved by changing the third and fourth paragraphs of Section 5.5 to the following: Because an X.509 certificate typically is valid several years, a mechanism to distribute certificate status information is necessary. CRL and OCSP are the two commonly used mechanisms. CAs that issue PIV Authentication, Card Authentication, digital signature, or key management certificates shall maintain a Hypertext Transfer Protocol (HTTP) accessible web server that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it, as specified in [PROF]. In addition, every CA that issues PIV Authentication or Card Authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues. PIV Authentication, Card Authentication, digital signature, and key management certificates shall contain the crlDistributionPoints extension needed to locate CRLs. PIV Authentication certificates and Card Authentication certificates shall also contain the authorityInfoAccess extension needed to locate the authoritative OCSP responder.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-47	DoD	Jonathan Shu	Technical	50	1576-1577	5.5.1	The Federal PKI is currently discussing possible changes to the overall architecture to streamline operations. Overly constraining the architecture and PKI requirements in FIPS-201 prevents the Federal PKI from implementing changes. Specific requirements for PKI should be addressed in [COMMON] rather than being overly specified in FIPS-201. Specific requirements for publication of CA certificates and CRLs should be addressed in [COMMON], not the SSP Repository Service Requirements document which is not applicable to Federal PKIs.	Recommend replacing the first sentence of section 5.5.1 with "This Standard requires distribution of CA certificates and CRLs. Specific requirements are found in [COMMON].	Decline to delete "using HTTP" from the first sentence of Section 5.5.1, as per DoD-45. Referencing [COMMON] rather than [SSP REP] in the second sentence of Section 5.5.1 would not be appropriate as [SSP REP] provides a level of detail about repository requirements that cannot be found in [COMMON].
DoD-48	DoD	Jonathan Shu	Crtical (General)	50	1578 - 1580	5.5.1	This section appears to infer any x.509 public key infrastructure (asymmetric cryptography) certificate that contains the FASCN or some representation of the FASCN cannot be made publically available. This requirement makes no sense when trying to use PKI as intended and supporting interoperability/cross recognition of PKI certificates amongst federal issuers. Public certificates must be public. It is not clear what the concern may be with the FASCN (as part of the CHUID) being within a public certificate, when the CHUID is a free read on contact and contactless interfaces of the PIV.	Strongly recommend deleting this requirement.	Declined See DoD-61 in disposition of comments for March 2011 Draft FIPS 201-2.
DoD-49	DoD	Jonathan Shu	Technical	55	1704	6.2.3.1	PKI-AUTH, per tables 6-2 and 6-3, can apply to physical or logical authentication. This section seems to apply to the physical authentication use case, but that's not specified. Much of the content in this section is not accurate/feasible for logical authentication.	Recommend revising the introductory sentence of section 6.2.3.1 to specify that this is for PKI-AUTH as used in physical access only, OR revise content to reflect both physical and logical authentication workflows. Consider using "relying party" terminology (which in the case of a PACS would be the reader) versus "reader".	Resolved by AMAG-32.
DoD-50	DoD	Jonathan Shu	Technical	56	1729	6.2.3.2	The Asymmetric Card Authentication Key provides the capability to sign an arbitrary value without requiring user activation. An attacker could potentially forge an email message, calculate the message digest, and have the aCAK sign the digest. Some protections exist (e.g., a critical EKU and absence of other allowed EKUs).	In recognition of occasional poor public key enabling by Relying Party, DoD recommends an additional protection whereby the card "prepends a salt" to the challenge to thwart such attacks. DoD will reiterate these concerns during the revisions of NIST SP 800-73-3.	Declined. See DoD-29.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-51	DoD	Jonathan Shu	Critical (Technical)	58	1775-1777	6.2.5	This section deprecates CHUID authentication method and, as such, expects all physical access control systems to be able to electronically authenticate PIV cardholders with a different mechanism in 5 years. This requirement will significantly impact DoD and is cost prohibitive. DoD has been activity working to migrate DoD installations towards using electronic authentication from the CAC PIV rather than separate proprietary PACS only badges and VIS (flash and pass). This activity is being done within existing budget circles and as systems are upgraded. The main technologies that have been prescribed to electronically facilitate access to DoD installations are the use of the full signed CHUID for CAC/PIV holders and barcodes for DoD ID cards in possession of DoD familiy members, retirees, or local visitors. This requirement would require DoD to quickly (as an out of band activity) implement the CAK (in which current CAC PIVs do not implement) and re-engineer PACS systems that have only recently been installed. This is a non-starter. Additionally, DoD understands the risks and plan to outline other techniques in conjunction with CHUID authentication to mitigate some of the risk (e.g., combination of VIS). The CHUID must remain beyond the 5 year window for this revision cycle of FIPS 201.	Do not deprecate CHUID authentication and maintain CHUID authentication at the level of "SOME confidence"	Declined. In order for the CHUID authentication mechanism to be considered to provide "SOME confidence" in the asserted identity's validity, it would have to have to satisfy requirements comparable to those specified for E-Authentication Level 2 in SP 800-63-1. In the CHUID authentication mechanism, the CHUID data element is used as a long-term shared authentication secret. One of the requirements for Level 2 in SP 800-63-1 is that "[l]ong-term shared authentication secrets, if used, are never revealed to any other party except Verifiers operated by the Credential Service Provider (CSP)." The CHUID data element does not satisfy this requirement.
DoD-52	DoD	Jonathan Shu	Critical (Technical)	43 and 63-64	1345 and 1945-1972	4.2.2 and B.2	This document continues to require PIV cards contain a NACI indicator. Since the original draft FIPS 201 of 2004, DoD has outlined its concern with the requirement to include a cardholder's background investigation status within fields of the PIV authentication certificate. DoD has been concerned with how this information would be updated to provide accurate information to Relying Parties. Our philosophy has been to facilitate the exchange of this information across agencies through backend attribute exchange transactions between cards issuers or have relying parties use the existing separate systems that contain up-to-date adjudicated background investigation to verify this information, if needed. DoD does not understand the return on investment to implement this change when the moment it is placed on the card. It could be inaccurate. Additionally, during the summer 2009, members of the Federal CIO Council's Identity Credentialing and Access Management Sub-committee (ICAM SC) agreed to remove the NACI indicator requirement from future revisions. This agreement should be reflected in FIPS 201-2.	Delete Section B.2 and all references to the PIV NACI indicator.	Declined. See DoD-48 in the disposition of comments for March 2011 Draft FIPS 201-2. In addition the FRN for FIPS 201-1 (http://www.itl.nist.gov/fipspubs/FR%2003312006PIV.pdf) states the need for an indicator: "This requirement [NACI indicator) is imposed to be consistent with the OMB memorandum M–05–24. The NACI indicator relays the rigor of identity proofing completed on the PIV cardholder when the card was issued. The relying parties, such as federal agencies, may require NACI completion to allow access to their resources. The NACI indicator will enable agencies to make an informed decision about the cardholders binding to the identity credentials." Note: FIPS 201-2 will note in Section 4.2.2 that other methods to indicate background investigation status will be explored in future revision of FIPS 201.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-53	DoD	Jonathan Shu	Technical	59	1812 - 1813	6.2.6	The description of VIS authentication could be improved.	Recommend changing "Human inspection of card, which is not amenable for rapid or high volume access control," to ""Human inspection of the card, which is not amenable for rapid or high volume access control and is susceptible to human error." And, changing "Resistant to use of unaltered card by non-owner of card," to "Some resistance to use of unaltered card by non-owner of card."	Accept
DOE HQ-1	DOE - HQ	T. Gaines	T	6	385	2.3	The potential for alternate biometrics is not even mentioned here in 2.3. In setting the stage for the use/potential use of an alternate biometric there should be at least some reference to the possibility and SP 800-76 that will establish the requirements for any alternate biometric. As it is section 2.3 and 2.4 seem to be misaligned.	Introduce alternate biometric options here as well as in section 2.4. Also clearly state that the alternate biometric is only useful for biometric authentication and is not a substitute for fingerprint submission in support of background investigations.	Declined. Section 2.3 specifies collection of biometric data for background investigations, and there currently is no alternative biometric options for this purpose. Section 2.4 specifies the collection of all other PIV biometric data.
DOE HQ-2	HS-53	M. Pekrul	T	21	482	2.7	There is no outside limit on the age of a NACI which may be used for PIV issuance. The authors have expressed the opinion that reinvestigative requirements are the business of OPM. However, OPM is considering these only from the view point of suitability for employment. The concern of this process is more to related whether an individual should be given a credential for access to physical spaces and logical systems. It would not be beyond the authority of NIST to prescribe an outside age limit such as 5 or 10 years.	Edit the sentence to read: "The process shall begin by locating and referencing a completed and favorably adjudicated NACI (or equivalent or higher) or Tier I or higher federal background investigation record which is no older than 5 years."	Declined. It would be inappropriate for NIST to impose more stringent background investigation requirements than those specified by OPM.
DOE HQ-3	DOE - HQ	T. Gaines	T	29	1084-1089	4.1.4.1	According to the text, the purpose of "Zone 15F—Color-Coding for Employee Affiliation. Color-coding shall be used for additional identification of employee affiliation as a background color for Zone 2F (name) as depicted in Figures 4-1 and 4-4. The following color scheme shall be used: + Blue—Foreign National + White—Government Employee + Green—Contractor." However, there are other "Affiliations" that are not "Contractors" "Government Employees" or "Foreign Nationals." Currenly all of these are given a "white" stripe the same as "Government Employees".	Recommendation: Zone 15F—Color-Coding for Employee Affiliation. Color-coding shall be used for additional identification of employee affiliation as a background color for Zone 2F (name) as depicted in Figures 4-1 and 4-4. The following color scheme shall be used: + Blue—Foreign National + White—Government Employee + Green—Contractor + Orange—Other Affiliation In any case it needs to be clear when a individual is not Fed, Contractor or Foreign National.	Declined. HSPD-12 specifies the issuance of PIV Cards to “employees and contractors (including contractor employees).” Similarly, OMB M-05-24 specifies requirements for the issuance of PIV Cards in terms of employees and contractors. If DOE needs for its PIV Cards to include addition information about the type of "affiliation" it may utilize the Zone 8F Employee Affiliation and/or the Zone 16F Photo Border.
DOE HQ-4	ORNL	J. Watson	T	60	1841-1848	6.3	No confidence: VIS, SOME CONFIDENCE PKI-CAK,CHUID	Enrollment process is validated, the CHUID is generated from the system, thus reliability should be more than No Confidence.	Declined. While an attacker who has not compromised a card management system cannot generate a fake CHUID whose signature would validate, the CHUID data element is available for free-read on the contactless interface, and it would be very easy for an attacker who had read the CHUID from a PIV Card to copy that CHUID onto a clone card, and then this clone card would be accepted by any system that only performed the CHUID authentication mechanism. Thus the authentication mechanism provides little assurance of the identity of the cardholder. Thus, it is most appropriate to indicate that the assurance level provided by the authentication mechanism is LITTLE or NO assurance (comparable to e-Authentication Level 1). See also SCA-86 and SCA-87 from the disposition of comments for March 2011 Draft FIPS 201-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOE HQ-5	DOE - HQ	T. Gaines	T	5 & 9	362-365 also 482-487	2.1 and 2.7	There is apparently some confusion about what constitutes "initiated" and credentials have apparently been issued based on the fact that a background investigation was requested. No follow-up was done & no NCHC results were obtained but the cards were issued. Further, there still does not appear to be a clear requirement for follow-up and confirmation that the NACI, equivalent or better is ever actually completed and satisfactorily adjudicated. If the NCHC is used the record is typically forgotten and never updated	1) Clarify "initiated" to assure rejected records are not used as the basis for credential issuance regardless of the subsequent time element 2) Require follow-up on records where the NCHC is used as the basis for credential issuance to assure the NACI, equivalent or better is actually completed and satisfactorily adjudicated and that the record is updated to reflect this completed	Resolved by OPM-8. Additionally, OPM will work with agencies to review processes and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications. Additional guidance can also be found at OMB's Memorandum M-05-24. 2) Resolved by adding the following footnote to the 2nd sentence of the third bullet of section 2.8 and to second paragraph, second sentence of section 2.9.1: The IDMS should reflect the adjudication status of each PIV cardholder.
DOE HQ-6	DOE - HQ	T. Gaines	T	12	616	2.9.1	The language provided states, "The issuer shall verify that the employee's or contractor's background investigation (BI) is valid before renewing the card and associated credentials." The exact position/role of the "issuer" in this case is not clear. Is it intended that "someone" in the "agency" must independently verify the BI status? Is there some expected position/process by which this should be done.	Please: Provide clarification and expectations here. If the goal is to assure an initiated BI has actually been completed, the words need to make that clear. We should also consider prohibiting renewal if the "NACI" is not final & approved. Otherwise there is no call for reinvestigation to support card issuance and therefore nothing to verify. Additionally, verifying the "status of the BI" does nothing to verify continued employment and the ongoing need for a credential. These status elements need to be verified also prior to renewal.	Resolved by replacing the 2nd sentence of the 2nd paragraph of the new Reissuance section (Section 2.9.1) which combines the renewal and re-issuance section: The issuer shall ensure that the proper authority has verified that the employee's or contractor's background investigation is valid before reissuing the card and associated credentials.
DOE HQ-7	DOE - HQ	T. Gaines	T	26 - 40	1030 - 1232	4.1.4	Specifications for PIV Credential topography should not be contained in FIPS 201. This is much too detailed and specific for the FIPS and may be subject to changes that should not wait on the review schedule for a FIPS.	Detailed specifications for this and other credentialing characteristics and capabilities should be placed in the appropriate Special Publication to assure that the requirements can be adjusted in a timely manner if and when needed.	Declined. NIST incorporated relevant and stable aspects of SP 800-104 into FIPS 201-2. Card topography has been stable since 2005 and NIST believes that it will not change very often.
DOE-1	DOE	Deborah Coote	T	All	All			In the definition of a common identity credential system, some key controls requirements of operational and managerial nature are not well defined. (See comment lines 6-10).	See resolutions to other DOE comments.
DOE-2	DOE	Deborah Coote	T	vii	Paragraph 10 / Line 202			Document says that implementation guidance to Personal Identity Verification (PIV) enabled Federal information systems/ physical facilities will be outlined in the "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance." In fact, Version 1 of this document is dated 11-10-09. Please make clear what version will outline guidance now and in the future, and give an expected date when the updated guidance will be made available. Reference www.idmanagement.gov. Please note that Version 1 does not contain any security considerations in Section 6.4. Security considerations are to be provided in version 2.	Out of scope. The FICAM Roadmap is developed by Identity, Credential, and Access Management Subcommittee (ICAMSC), not by NIST.
DOE-3	DOE	Deborah Coote	T	viii	Paragraph 11 / Line 216			Document says it is the implementer's responsibility to ensure that components, interfaces, communications, storage media, managerial processes, and services used within the identity verification system are designed and built in a secure manner. How is this to be tested? How financially independent of the assessed is the assessor? Can the assessor have a conflict of interest?	Out of Scope. FIPS 201 specifies functionality, interoperability, and security requirements for PIV Credentials in response to HSPD-12. There are additional standards and guidance that implement FISMA. Many of these individual system security requirements are outside the scope of FIPS 201.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOE-4	DOE	Deborah Coote	T	10	Line 527	2.7		How will the PIV process be tested for adherence to segregation of duties in the process used to issue the credential? Can the assessor be employed by/paid by the assessed?	Declined. See SP 800-79 for conformance requirements related to "segregation of duties".
DOE-5	DOE	Deborah Coote	T	54		6.2.1.1 & 6.2.1.2		Please describe the characteristics of BIO and BIO-A. What are the differences in their characteristics?	Noted. The characteristics of BIO and BIO-A are listed in Section 6.2.1 and the difference between them is described in Section 6.2.1.2. See also Cert-6.
DOE-6	DOE	Deborah Coote	T	56	Line 1717	6.2.3.1		Please add to the list of characteristics of the Public Key Infrastructure (PKI)-based authentication mechanism that the PKI-PIV Authentication Key (PKI-AUTH) provides protection against use of a revoked card.	Accept
DOI-1	Department of the Interior	Dwayne Pfeiffer, tel	T	29	1084-1089	4.1.4.1	According to the text, the purpose of "Zone 15F—Color-Coding for Employee Affiliation. Color-coding shall be used for additional identification of employee affiliation as a background color for Zone 2F (name) as depicted in Figures 4-1 and 4-4. The following color scheme shall be used: + Blue—Foreign National + White—Government Employee + Green—Contractor." However, There are "Employee Affiliations" other than "Contractors" that are not "Government Employees", therefore, I recommend that the color Green be specified for all "Non-Government Employees".	Zone 15F—Color-Coding for Employee Affiliation. Color-coding shall be used for additional identification of employee affiliation as a background color for Zone 2F (name) as depicted in Figures 4-1 and 4-4. The following color scheme shall be used: + Blue—Foreign National + White—Government Employee + Green—Non-Government Employee	Declined. FIPS 201 is responsive to HSPD-12, which is specific "employees and contractors (including contractor employees)". The green color code, therefore, should be specific to "contractors and contractor employees" Under OMB M-05-24, other government affiliates are listed as employees.
DOJ-1	DOJ	Eric Olsson	G	12 (Tracked changes version)	582	2.8.2 Grace Period	The grace period allows agencies to issue employees or contractors new PIV cards after brief lapses in employment, however, no term is specified. A maximum term should be specified so agencies can better rely on existing chains-of-trust or biometric records from other agencies utilizing the same shared service or the biometric records from another agency.	A two year maximum is suggested for lapses in an employee or contractor employment or contracting activity.	Resolved by OPM-28.
DOJ-2	DOJ	Eric Olsson	G	16	752	2.9.5	The PIV Card shall be terminated under the following circumstances: an employee of a Federal contractor separates (voluntarily or involuntarily) from his or her employer. Contractors often move from one contracting company to another contracting company and continue work at that agency with full knowledge of the agency. DOJ has specifically designed the card topology to support Component transfers and the like. It is costly to terminate and re-issue a PIV Card when a contractor changes companies or Components within the agency with little or no break in service. Additionally, contractors that no longer require a PIV Card are handled under the next PIV Card termination bullet which reads, "The PIV Card shall be terminated under the following circumstances: a contractor changes positions and no longer needs access to Federal buildings or systems."	Agencies should have the leeway to continue using the original PIV Card without termination when a contractor continues service at the agency but changes contracting firms.	Resolved by deleting the second bullet in Section 2.9.5 (now Section 2.9.4).
DOS-1	DOS/DS/ST	MSulak	G	10	540	2.8	It appears that this section is stipulating that the Head (Secretary) or Dupty Secretary (or equivalent) is now the DAA of the department or agency.	Change the wording in (or equivalent) to read (or delegate). This will allow an Assistant Secretary or Dupty Assistanct Secretary to be the DAA.	Resolved by DoD-10.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOS-2	DOS/DS/ST	MSulak	G	11	570	2.8	The last sentence appears to conflict with the definition of a card issurer, the person that physically creates the card and hands it to the applicant and the PCI.	Change the sentence to read "The PIV Card Issuer Facility (PCIF) Manager is responsible for the card stock……"	Declined. The PIV Card Issuer (PCI) is an entity or an organization, made up of many individual, that is responsible to issue PIV Card. PIV Card Issuer is not a single individual or a role. FIPS 201-2 does not name specific roles because this will vary from agency to agency.
DOS-3	DOS/DS/ST	MSulak	G	31	1159	4.1.4.3	Zone 22F only provides for the indication of the card orientation towards meeting the requirements of Section 508 but does not address the ability of determining the expiration date of the card.	Add the capability of indicating the expiration date of the card in this location for individuals with a visual impairment under Section 508.	Declined. Zone 22F is provided specifically for tactile markers for card orientation using laser engraving technology. This technology is choosen because it does not interfere with the internal antenna(s) and is not suitable for generating readable information for vision-impaired cardholders. The expiration date of the card may be obtained from the CHUID data element on the card.
DOS-4	DOS/DS/ST	MSulak	E	52	1609	6.1	Parts of the section appear to be redundent with that of section 6.1.1 and leaves the reader confused in the intent of the two sections.	Remove lines 1609 to 1620 of section 6.1.	Declined. Section 6.1 describes the four PIV assurance levels. Section 6.1.1 then compares those levels to the assurance levels defined in OMB memorandum M-04-04.
DOS-5	DOS/DS/ST	MSulak	G	57	1757	6.2.4	This bullet is not correct the way it is worded. A revoked card, even with a symmetric key, will not be able to gain access to a facility because the access control system will have it locked out of the system. It will not provide protection against a revoked PIV Auth Cert.	Change the wording of this bullet to read "Does not provide protection against use of a revoked card Certificate.	Declined. Section 6.2.4 correctly states that the SYM-CAK authentication mechanism does not provide protection against use of a revoked card. As noted in the comment, this may not be a security vulnerability if the access control system has de-authorized use of the card.
DOS-6	DOS/DS/ST	MSulak	G	57	1761	6.2.5	The use of the words "Logical Credential" is misleading and can give the impression that the CHUID is used for logical access.	Change the wording of the sentence to read "The PIV Card provides a mandatory container called the CHUID. This will conform to SP 800-73-3 definition.	Resolved by revising the sentence from: "The PIV Card provides a mandatory logical credential called the CHUID." to "The PIV Card provides a mandatory data element called the CHUID."
DOS-7	DOS/DS/ST	MSulak	G	58	1773	6.2.5	This bullet is not correct the way it is worded. A revoked card, even with a symmetric key, will not be able to gain access to a facility because the access control system will have it locked out of the system. It will not provide protection against a revoked PIV Auth Cert.	Change the wording of this bullet to read "Does not provide protection against use of a revoked card Certificate.	Resolved by DOS-5.
DOS-8	DOS/DS/ST	MSulak	E	59	1817	6.3	The flow of the document is in consistant with the text of this section. We should not be discussing authenntication machanisms before we outline the assurance levels.	Reverse section 6.3 (and all subsections) with that of section 6.2 (and all subsections).	Declined. The current order is correct since terms used in Section 6.3 must be defined first. Section 6.2 defines the terms and provides details. While Section 6.3 uses these terms.
EPA-1	EPA	Edna Reynolds	E			2.9.1.1	1) The requirement states that the card issuer shall issue the cardholder a new card when evidence of a formal name change is presented to the card issuer. Please confirm that the card issuer is the agency PIV system and not the PIV Issuer role player. And that it is not a requirement for the PIV Issuer role player to provide a new card when evidence of a name change is presented directly to them. Rather, that the cardholder may present the evidence of a name change directly to the authoritative source so that the PIV Issuer will issue the new card after the changed name is updated by the authoritative source.		As noted in DOS-2, PIV Card Issuer is an entity or an organization responsible for issuance of PIV Cards. This entity (PCI) may or may not, completely or partially, outsource the issuance process; however, the PCI is responsible to meet the requirements of FIPS 201-2. See also SP 800-79 for further details.
EPA-2	EPA	Edna Reynolds	E			2.9.1.1	2) We are seeking clarity on what is needed to produce a new card with an expiration date that is later than the expiration date of the original PIV card. Must everyone be re-investigated to get a card with a later date? Or may the agency simply confirm that an investigation is current, per OPM guidance.		FIPS 201-2 states that "a re-investigation is performed if required, in accordance with OPM guidance." Thus, a re-investigation only needs to be performed if OPM guidance requires that one be performed.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
F-1	Factor 3 Technologies	Greg McGregor	G	24	949, 950	4.1	To avoid creating two competing PIV Standards one for current Smart Card based on FIPS 201and one for extended Smart Cards with System on Card functionality we propose a minor alteration to the orientation diagrams and references. This only affects areas specified to be optional areas designated for use by the manufacturer. In a 'system on card' device the electronic contacts, electronic display, and fingerprint area sensor should be present on the same side of the card. This proposed change does not alter current manufacturing processes. This proposed allowance for the PIV Card complies fully with physical characteristics as described in International Organization for 957 Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373 958 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards 959[ISO14443]. The other alternative is to form a new standard for an ISO System on Card PIV not based on FIPS 201-2. This should not be necessary as slight changes can accommodate System on Card that affect optional areas by the manufacturer and enables full compatibility with all existing card readers. This does not change any mandatory areas it only affects optional areas.	Change verbiage to: "References to the front of the card apply to the side of the card that contains the Mandatory Items defined in Section 4.1.4.1.	Declined. FIPS 201 is the Standard for PIV, so there is no risk that there will be two competing PIV Standards. The purpose of FIPS 201 is to specify a "Common Identification Standard for Federal Employees and Contractors." Allowing for the proposed flexibility in card design would not further the goal of a common identification standard.
F-2	Factor 3 Technologies	Greg McGregor	G	25	1007	4.1.3	Following the feedback we have received from the visually impaired testers, for system on card users we want to make sure the (physical indicator) notch is on the same side as the smart chip to guide proper insertion of a card to a reader. This maintains compliance with System on Card, ISO 7816 and proper insertion into a standard card reader. Allowing the proposed change will provide a indication of proper card orientation without impacting mandatory information required on the card. This only affects areas specified to be optional areas designated for use by the manufacturer and enables full compatibility and ease of use to the visually impaired when using existing card readers.	Change references for proper card orientation indicators to a specific side (Section 4.1.4.3) of the card for it to be on the same side as the electronic contacts.	Resolved by F-1.
FPKI-1	FPKI CPWG	CPWG	T				Currently, FIPS 201-2 has a number of references to specific technical details that appear in "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON] (e.g., See comments DHS-8 (CRL Issuance Frequency), Cert-99 & DoD-59 (Optional use of LDAP). To allow for policy changes that accommodate new and emerging technologies (e.g., mobile devices), the FPKI CPWG recommends that FIPS 201-2 expand references to [COMMON] for any PKI technical details to satisfy FIPS 201 requirements. Specifically, FIPS 201 requirements could be written at a higher level such that it defers any PKI technical specifications to [COMMON] (e.g., technical details related to policy OIDs or use of EKUs). This will allow the FPKI more flexibility for complying with FIPS 201 requirements as the policy evolves to meet the needs of the FPKI Community without contradicting FIPS 201.	Revise all FIPS 201-2 paragraphs related to PKI technical specifications to reference "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON].	Declined. As the scope of the Common Policy is not limited to PIV Cards, FIPS 201-2 needs to include information about which certificate policies may be used to issue the different types of certificates needed for PIV Cards, as well as other PIV-specific information. Care has been taken to ensure that any PKI-related requirements specified in FIPS 201-2 are unlikely to need to be changed before the next revision of the Standard. Also resolved by DoD-36, DoD-37, DoD-45, DoD-46, and DoD-47.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FPKI-2	FPKI CPWG	Tim Baldridge	T		460-475	2.6	Cost savings and efficiencies may be achieved by accepting approved PIV-I issuers enrollment data that is the PIV-I issuer chain-of-trust, excluding any the background investigation data which is intrinsically Governmental for PIV	(Following line 455) Approved PIV-I issuer chain-of-trust data may be used by Federal Departments and Agencies for issuer identity proofing in meeting PIV registration requirements. A PIV-I issuer chain-of-trust shall include the enrollment and forensic data with respect to the PIV-I card issued to the new PIV applicant. A PIV-I issuer chain-of-trust shall not include background investigation data which is intrinsically Governmental for PIV. PIV-I issuers providing chain-of-trust data to PIV card issuers shall have available for inspection evidence of a qualified independent assessment of the PIV-I issuer adoption and use of and approved identity proofing and registration process in accordance with [SP 800-79]. (Following line 475) PIV-I for identity proofing: A Federal contractor working for a company where a PIV-I card is used as the company identification badge enters a new assignment that requires a PIV card. The contractor responds to an invitation for a PIV card application through a portal secured by the PIV-I card and authorizes the release of the PIV-I card issuer chain-of-trust data to the PIV card issuer. The PIV-I chain-of-trust data, including complete identification data, biometric images and templates, images as evidence of primary identity source document inspection, etc., is released to the PIV card issuer based on the applicant's approval. The PIV card issuer uses the biometrics and source documents from the PIV-I Issuer chain-of-trust. Upon completion of the background investigation in Section 2.7 and a cardholder 1:1 biometric match to connect to the PIV issuer's new chain-of-trust to the cardholder the PIV card issuer proceeds to issue a new card as described in Section 2.9.2	Declined. As PIV-I issuers are not subject to Federal requirements, the PIV-I identity proofing and registration process cannot be accepted as an alternative to the PIV identity proofing and registration process.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FPKI-3	FPKI CPWG	CPWG	T		1278-1281		The FPKI CPWG requests that FIPS 201 allow CMS certificates to be issued under the PIV Content Signing Policy OID.	Change: "The public key required to verify the digital signature shall be provided in the certificates field of the 1278 CMS external digital signature in a content signing certificate, which shall be an X.509 digital signature 1279 certificate issued under the id-fpki-common-devicesHardware, id-fpki-common-hardware, or id-fpki-1280 common-High policy of [COMMON]." to: "The public key required to verify the digital signature shall be provided in the certificates field of the 1278 CMS external digital signature in a content signing certificate, which shall be an X.509 digital signature 1279 certificate issued under the id-fpki-common-piv-contentSigning, id-fpki-common-devicesHardware, id-fpki-common-hardware, or id-fpki-1280 common-High policy of [COMMON]."	Resolved by changing the text to say: "For signatures created before October 15, 2015, the public key required to verify the digital signature shall be provided in the certificates field of the CMS external digital signature in a content signing certificate, which shall be an X.509 digital signature certificate issued under the id-fpki-common-piv-contentSigning, id-fpki-common-devices, id-fpki-common-devicesHardware, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON]. For signatures created on or after October 15, 2015, the public key required to verify the digital signature shall be provided in the certificates field of the CMS external digital signature in a content signing certificate, which shall be an X.509 digital signature certificate issued under the id-fpki-common-piv-contentSigning policy of [COMMON]."
G-1	Gemalto	R. Outland	G				Related to PKI-CAK, PKI-AUTH, BIO, will the departments educate their employees about the increased times it will take to authenticate the card holder?		Noted. This is a question for individual departments.
G-2	Gemalto	N. Pattinson	G	8	472	2.4	The cost of PIV cards will increase to meet the extended lifespan to six years.		Out of Scope.
G-3	Gemalto	J. McLaughlin	E	57	1800	6.2.5	Spelling error "aIf"	Change to "if"	Noted. This comment is referring to the first draft of FIPS 201-2. The error has already been corrected in Revised Draft FIPS 201-2.
G-4	Gemalto	J. McLaughlin	G				The publication relies on associated special publications (e.g. SP 800-73, -76, 78, -96, etc.) to provide the technical details on new features introduced with this version. However, vendors can not implement nor can products be validated for listing by the GSA until the required Special Publications are updated and test procedures implemented by the certification bodies.	Provide the draft Special Publication updates and requisite test tools for comment by the time FIPS 201-2 is released as final to facilitate a reasonable development, test suite implementation, and commercialization cycle.	Declined. Draft Special Publication updates and requisite test tools will be made available for comment when they are available. It is not necessary to hold up publication of FIPS 201-2 until these documents are ready to be made available for comment. See also DHS TWIC-1, IBIA-2
IBIA-1	IBIA	Walter Hamilton	G		N/A		FIPS 201-2 describes functionality that is to be detailed in future releases of special publications. An example includes the virtual contact interface. FIPS 201-2 should not become effective before these special publications are finalized. It would be helpful if NIST could release a draft of SP 800-73 and other dependent publications before finalizing FIPS 201-2	Release draft of related special publications that implement new functionality described in FIPS 201-2 before finalizing FIPS 201-2.	Resolved by G-4. As noted in the Effective Date text, new features of the Standard, which are optional to implement, will not become effective until the release of the new or revised Special Publications upon which they depend.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IBIA-2	IBIA	Walter Hamilton	T	46	1424	4.2.3.3	This states that biometric data stored on the card may optionally be readable through the virtual contact interface after presentation of a valid PIN. FIPS 201-2 further states that the virtual contact interface will be defined in SP 800-73. It would be preferable to not restrict the ability to read the biometric over the virtual contact interface without a PIN as long as a trusted communciation session between the card and the reader has been established. While the next revision to SP 800-73 may or may not define a mechanism where the card can trust the reader, it is conceivable that such a capability could be added to SP 800-73 prior to the next five year cycle review of FIPS 201.	Change line 1424 and 1425 to read as follows: "…may optionally be readable through the virtual contact interface and after the presentation of a PIN. A PIN is not required if the communication session established between the card and the reader provides for a capability to ensure that the reader can be trusted by the card in a manner that is in accordance with [SP 800-73]."	Resolved by DHS TWIC-18.
IL-1	Intercede Ltd	Chris Edwards	E	7	425	2.5	The mixed use of Match Off Card, Match-on-Card, On-card comparison and Off-card-comparison is confusing and conflicts with established acronyms. MOC is almost universally understood to mean match-on-card.	Use only one term for each of these cases. Either pick something new or use existing industry norms for the acronyms. For example, MOC (or MOnC) for Match-on-card, OCC (or even OffCC)	Noted. Revised Draft FIPS 201-2 consistently uses the term on-card biometric comparison (OCC).
IL-2	Intercede Ltd	Chris Edwards	G	6	402	2.4	Allowing the same fingers to be used for MOC and OCC risks allowing an extractable authenticator. (The existing PIV templates can be read from an open card on a compromised computer and subsequently used to authenticate to it. Unlike the PIN, this cannot be changed easily)	Advise that the same fingers must not be used for both purposes.	Resolved by AMAG-5.
IL-3	Intercede Ltd	Chris Edwards	G	11	557	2.8	The requirement for a 1:1 bio match BEFORE THE CARD IS PROVIDED TO THE APPLICANT means that self-service activation is not possible. Existing processes may deliver a locked card to the applicant, who can then use a self-service application to perform a bio match against their enrolment record before unlocking the card and performing the secondary match against the template on card.	Change the wording to read 'Before a fully enabled card is provided to the applicant…" or something similar to permit locked, partially personalized cards to be delivered and activated remotely.	Declined. The requirement for a 1:1 biometric match also appears in FIPS 201-1, so existing PIV processes already need to satisfy this requirement. Furthermore, in order to be consistent with the requirements for Level 4 in SP 800-63-1, it is necessary to require the applicant to appear in person at each step in the identity proofing and registration process and to have the applicant identity himself/herself at each step in the process through the use of a biometric.
IL-4	Intercede Ltd	Chris Edwards	G	15	721	2.9.4	Kiosk-based PIN reset should permit 1:1 bio match against the cardholder's enrolment record as the means of authentication. Off-card bio match cannot be performed without first unblocking the PIN to read the bio template, so some user authentication is needed before this is done.	either an on-card, off-card or enrolment record 1:1 biometric match'	Resolved by changing sentence beginning on line 721 from: PIN reset at an unattended issuer-operated kiosk shall ensure that the cardholder's biometric matches the stored biometric on the PIV Card, through either an on-card or off-card 1:1 biometric match, and that the PIV Card is authenticated. To: PIN reset at an unattended issuer-operated kiosk shall ensure that the PIV Card is authenticated and that the cardholder's biometric matches either the stored biometric on the PIV Card, through an on-card 1:1 biometric match, or biometric data stored in the chain-of-trust, through a 1:1 biometric match.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IL-5	Intercede Ltd	Chris Edwards	G	15	725	2.9.4	Is there any reason to disallow the same biometric authenticated PIN unblock protocol that the kiosk performs?	Allow biometrically authenticated PIN unblock on a general platform, rather than limiting it to dedicated kiosks.	Declined. Use of biometric authentication at an issuer-operated kiosk is comparable to local authentication, since the issuer can ensure that the biometric sample being provided is coming from a biometric capture device, and is not simply a stored value that is being transmitted to the issuer. The issuer may also make use of biometric capture devices that include liveness detection capabilities. Biometric authentication from a general computing platform would be a form of remote authentication, which is not supported by SP 800-63-1. SP 800-63-1 does, however, support the use of biometrics to "unlock" a conventional authentication token, which is the manner in which biometrics are permitted to be used in the reset procedure from a general computing platform. The reset procedure from a general computing platform is strengthened by the requirement for an out-of-band authentication procedure, which is needed to account for the lack of control over the source of the biometric sample.
IL-6	Intercede Ltd	Chris Edwards	G	15	738	2.9.4	It is useful to be able to refresh fingerprints to allow for the gradual change over time. Matching the previously stored reference templates and then updating them is a reasonable operation. This would also apply if the person had a damaged finger originally for example. This is more reliable than the alternatives being suggested in the absence for Iris for example. It could also be easily bypassed by two successive resets - I used current fingers to add Iris, then use Iris to update fingers. The restriction is therefore a bit pointless.	Allow refresh of the same biometric by matching against the old set.	Declined. The verification data reset procedure is intended to address the case in which the retry counter for the on-card biometric comparison data has become zero, not to address routine refresh of verification data in cases where that authentication mechanism to the card has not already been blocked.
IL-7	Intercede Ltd	Chris Edwards	G	20	865	3.1.1	The distinction between a card reader and a card writer doesn't really exist. In order to read from a card, APDU commands are set to it and data is returned. This is indistinguishable from a data write operation.		Noted. FIPS 201 tries to draw the difference between the use of readers in relying systems environment and card issuance system environment.
IL-8	Intercede Ltd	Chris Edwards	G	21	892	3.1.2	There are a number of tasks assigned to the Key Management System that more naturally fall under the remit of the Certification Authority. These can be separate systems.	State that the CA is responsible for certificate management and status dissemination and that the KMS is resonsible for the secure storage and use of private (or symmetric) keys that are not generated on-card.	Declined. The CA is one part of the key management component. Key escrow services may be another part of the key management component.
IL-9	Intercede Ltd	Chris Edwards	G	29	1094	4.1.4.1	The use of letters to indicate the color, rather than the meaning of the color has always puzzled me. Surely it would be better to have C for Contractor, E for Federal Employee and F for Foreign National, rather than have to remember the color-role mapping as well? What is the purpose of telling a color-blind person that the band is Green, if they still have to work out what that actually means? Adding "W" for white seems unnecessary, as this is unaffected by colorblindness.		Declined. The abbreviations "B" and "G" for Blue and Green have already agreed upon and established in SP 800-104. Changing the abbreviations to "F" and "C" would cause confusion, since there are already many cards in use with either a "B" or "G." See also DoD-24.
IL-10	Intercede Ltd	Chris Edwards	G	48	1504	4.4.4	How can the PIN be 'transmitted securely and directly to the PIV card for card activation' when there is no means of securing this communication channel?		This requirement has remained unchanged from FIPS 201-1. A communication channel may be considered secure even if the data transmitted over it is not cryptographically protected. For example, a USB cable connecting a contact card reader to the computer into which the PIN has been entered could be considered a secure communication channel, as it would be difficult for an attacker to eavesdrop on this communication channel without being detected.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIH-1	National Institutes of Health (NIH)	Mr. Richie Taffet	General, Editorial and Technical	Page 29 - Zone 15F - Color Coding for Employee Affiliation	Line 1087 - Blue - Foreign Nationals	Section 4.1.4.1.- Mandatory Items on the Front of the PIV Card	The National Institutes of Health (NIH) is concerned with the change in the revised draft of the Federal Information Processing Standard (FIPS)-201-2, dated July 2012, requiring a blue stripe designation for foreign nationals. In the current standard (FIPS-201-1) use of a "blue stripe" to designate a foreign national is 'optional". NIH firmly believes the conditions underlying the rationale for requiring a "blue stripe" to visually identify foreign nationals in the work place do not exist at this agency and possibly others. The open collaborative nature of the NIH's biomedical and clinical research mission include many foreign nationals working side by side with their U.S. national counterparts. There is no national security or classified research projects conducted by NIH researchers that would require restrictive access privileges based or national origin or affiliation. Consistent with NIST's long-standing recognition that security and privacy controls should be implemented based on risk-based assessments, maintaining the "blue stripe" as an optional field each agency could make a risk based decision on whether or not visual distinction between members of the workforce who are foreign nationals is in the agency's best interest. In reviewing all of the 223 pages of comments that the National Institute of Standards and Technology (NIST) received during the initial comment period on the draft FIPS-201-2 standard, no agency or department requested making the "blue stripe" a mandatory field. At the July 25, 2012 NIST Workshop on the Revised Draft of FIPS-201-2, an NIH representative asked the panel for the rationale behind changing the blue stripe from optional to mandatory; the NIST panel members were unable to account for the change. A panel member did however refer the NIH representative to their Special Publication (SP) -800-104, "A Scheme for PIV Visual Card Topography". In reading over SP-800-104, dated June 2007, under Section 1:2 does not provide justification it states: "The purpose of this document is to provide additional recommendations on the Personnel Identity Verification (PIV) Card color-coding for designating employee affiliations. Compliance with this document is voluntary; (emphasis added)." "This document (SP-800-104) is not intended to contradict requirements specifically identified in the Federal Information Processing Standard 201 (FIPS 201) or its associated documents, nor limit options permitted by FIPS 201 except as explicitly stated herein. Clearly FIPS-201-1 allowed agencies and departments the option to identify, or not, foreign nationals with a "blue stripe" on their PIV cards. There appears to be no specific rationale proposed by NIST to mandate the requirement as stated in the revised draft FIPS-201-2. The NIH recruits a large number of foreign nationals to meet its biomedical research missions. Mandating that their PIV cards be designated with a "blue stripe" would appear by some international partners as discriminatory. Such a practice could hinder NIH's ability to recruit and maintain these invaluable assets to the nation's biomedical research endeavors and/or to NIH's leading edge clinical studies which include many foreign nationals.	The blue stripe indicating a foreign national should remain "optional" for Departments and Agencies with a need to visually identify foreign nationals.	Declined. As discussed with OMB, compliance with SP 800-104 has become mandatory since it is OMB's policy that (other than for national security programs and systems) agencies must follow NIST guidance (http://csrc.nist.gov/groups/SMA/fisma/compliance.html). Note: Departments and agencies are required to accept PIV Cards issued by other federal agencies. So, departments and agencies with a need to visually identify foreign nationals need this information to be on all PIV Cards, not just the PIV Cards that they issue.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIH-1 (cont'd)							In addition, based on accreditation requirements of Joint Commission on Accreditation and Healthcare Organizations (JCAHO) all NIH's Clinical Center health care providers wear a badge with a blue stripe identifying them by name, with a current color photograph and denoting their health profession, i.e., physician, nurse, therapist, social worker, pharmacist, etc. The "blue stripe" field meets the Joint Commission requirements and to allow our patients and patient escorts to easily recognize who is a health care provider (and who is not). Mandating that PIV cards worn by foreign nationals which also contains a name field with a "blue stripe" would add confusion to our patient population and possibly endanger Joint Commission accreditation NIH fully understands the requirement for some agencies involved with classified information, systems or operations to visually identify foreign nationals In their workforce. The conditions making the blue stripe relevant for other agencies do not apply to the mission of the NIH. In the absence of clear linkage to a rationale for mandating use of the blue stripe designation NIH strongly recommends keeping this field as optional.		
NIH-2	National Institutes of Health (NIH)	Mr. Richie Taffet	General, Editorial and Technical	Page 29 - Zone 18F - Affiliation Color Code	Line 1094 - Affiliation Color Code	Section 4.1.4.1.- Mandatory Items on the Front of the PIV Card	Same as comment above	The blue stripe indicating a foreign national should remain "optional" for Departments and Agencies with a need to visually identify foreign nationals.	Resolved by NIH-1.
OPM-1	OPM-FIS	Tammy Paul (Operational Policy)	General	vi	136	6	Sensitive threats can come from both inside and outside the contiguous United States. It seems the real intent of this section is to emphasize exceptions when outside the US, regardless of where the threats originate.	Delete "from"	Resolved by replacing the sentence starting in line 136 with: For cardholders with particularly sensitive threats while outside the contiguous United States, the issuance, holding and/or use of PIV cards with full technical capabilities as described herein may result in unacceptably high risk.
OPM-2	OPM-FIS	Tammy Paul (Operational Policy)	Technical	vii	172		"unclassifiable fingers" It is the print that is unclassifiable, not the fingers.	"fingers" > "fingerprints."	Accepted.
OPM-3	OPM-FIS	Tammy Paul (Operational Policy)	Technical	viii	210		assurance provided by the issuer of an identity credential that the individual in possession of the credential has been correctly identified; It seems the key point here is the VERIFICATION of that identity.	assurance provided by the issuer of an identity credential that the identity of the individual in possession of the credential has been correctly verified;	Declined. Verification of identity is required for the issuer to provide assurance that the individual has been correctly identified, but it is the means, not the goal.
OPM-4	OPM-FIS	Tammy Paul (Operational Policy)	General	1		1, 1.1	These sections emphasize "authentication" with no mention of the verification process (i.e., investigation process) which must first occur. Verification processes must occur before a card is produced and available to authenticate.	Add reference to verification.	Declined. NISTIR 7298 defines authentication as "Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system." The verification process described in the comment is covered in the Introduction as part of "the process used to issue the credential."
OPM-5	OPM-FIS	Tammy Paul (Operational Policy)	General	5	351	2	"[HSPD-12] established control objectives for secure and reliable identification of…" This is an opprtunity to emphasize the identity is verified.	[HSPD-12] established control objectives for secure and reliable identity verification of…	Declined. Section 2.1 already states that ensuring that credentials are "issued based on sound criteria for verifying an individual employee's identity" is one of the control objectives for secure and reliable identification of Federal employees and contractors.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OPM-6	OPM-FIS	Tammy Paul (Operational Policy)	General		362-365	2.1	FIPS 201 does not have authority to provide the investigative and adjudicative processes for physical and logical access to federal facilities and information systems. As the Suitability Executive Agent under EO 13467, OPM is the authority which develops and implements uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability and eligibility for logical and physical access to federally controlled facilities or information systems. Furthermore, there is no distinction in FIPS 201 between an interim and a final credential. One problem is that it could be interpreted that that an interim credential based on only on a NCHC could be used by the cardholder indefinitely because an investigation had been "initiated," a term in investigations processing but undefined here in FIPS 201 and out of scope. An interim PIV cannot be used indefinitely. It can only be used until the results of the background investigation have returned and a credentialing (adjudicative) determination has been made. In addition, background investigations have their own timeliness standards. Agencies must submit their adjudicative determinations to the SII/CVS system. There are timeliness requirements for submitting those decisions, which while being out of scope for FIPS 201, could have implications for physical processing requirements for the cards.	Delete lines 362-365. Alternatively, ensure all language is current, coordinated and consistent with OPM's policies on investigations and adjudications. Due to ongoing reform efforts in the personnel security community, special attention should be placed on the term "current."	Declined. The requirements are consistent with M-05-24 and the federal investigative standards.
OPM-7	OPM-FIS	Tammy Paul (Operational Policy)	General	5	362-365	2.1	FIPS-201 does not address the distinction between interim and final credentials. This is a gap that needs to be addressed. As FIPS 201 is written, a final credential could be issued after the completion of the NCHC portion of the background investigation. The issuance of a final PIV credential based only on the results of the NCHC portion of a NACI would be inconsistent with OPM's Final Credentialing Standards. Only an interim PIV card may be issued if the NACI has not been completed. This gap between interim and final credentials is problematic because line 2018 defines a credential as the PIV Card.	Coordinate additional text regarding interim and final credentials with OPM. Change to "An interim credential is issued only after a National Agency Check with Written Inquiries (NACI) (or equivalent or higher) or Tier 1 or higher federal background investigation is initiated and the Federal Bureau of Investigation (FBI) National Criminal History Check (NCHC) portion of the background investigation is completed. A final credential is issued only after the federal background investigation is completed."	Declined. No interim PIV card is specified in FIPS 201. PIV Cards that are issued before the federal background investigation is completed satisfy the requirement from OMB Memorandum M-05-24 that "Identity credentials issued to individuals without a completed NACI or equivalent must be electronically distinguishable (i.e. information is stored in the data on the card) from identity credentials issued to individuals who have a completed investigation." There is no requirement to issue a new PIV Card or to update the credentials on the existing PIV Card when the background investigation is completed. FIPS 201-2 does, however, state that "The PIV Card shall be revoked if the results of the background investigation so justify."
OPM-8	OPM-FIS	Tammy Paul (Operational Policy)	General	5	363	2.1	the initiation of a federal background investigation is not defined in FIPS 201, but it may make it easier on agencies if it is (informative--because it is out of scope for FIPS 201)	the initiation of a background investigation should be defined as the submission of the investigative request via e-QIP to OPM or other Federal background investigation service provider	Resolved by inserting the following footnote: The initiation of a background investigation is defined as the submission of the investigative request to OPM, or other Federal background investigation service provider (if authorized).

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OPM-9	OPM-FIS	Tammy Paul (Operational Policy)	Technical	5	369	2.1	*A person suspected or known to the government as being a terrorist is not issued a credential.* This statement may require a footnote- **if OPM determines that both FBI checks must be completed in order to determine possible terrorist ties. Note, page 2 of the Springer memo says "A PIV card will not be issued to a person if... The individual is known to be or resonably suspected of being a terrorist, Footnote 4." Footnote 4 says, "OPM's background investigation includes checking names against the FBI's *investigation files*". (This implies the C0 Namecheck, NOT JUST the B0 Fingerprint.)**	Ensure language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Noted and discussed with OPM.
OPM-10	OPM-FIS	Tammy Paul (Operational Policy)	General	6	380	2.2	OPM issued Final Credentialing Standards, not guidance.	Change to " Federal departments and agencies shall use the credentialing standards issued by the Director of the Office..."	Resolved per OPM by replacing: "Federal departments and agencies shall use the credentialing guidance issued by the Director of the Office of Personnel Management (OPM) to heads of departments and agencies when determining whether to issue or revoke PIV Cards (e.g., [SPRINGER MEMO], [FIS]). In addition to OPM's [FIS], Federal department and agencies shall also apply credentialing requirements specified in applicable OMB memoranda (e.g., OMB Memorandum M-05-24 [OMB0524]" With: "Federal departments and agencies shall use the credentialing guidance issued by the Director of the Office of Personnel Management (OPM)1 and OMB2. " Footnotes: 1. For example, [SPRINGER MEMO] at http://www.opm.gov/investigate/resources/final_credentialing_standards.pdf and the Federal Investigative Standards 2. For example, [OMB0524] at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf
OPM-11	OPM-FIS	Tammy Paul (Operational Policy)	Editorial	6	382	2.2	OPM will not be issuing the new Federal Investigative Standards by itself. It will be a joint issuance with ODNI.	Remove "OPM's" and replace with "the" as in "the Federal Investigative Standards."	Resolved (with OPM) by OPM-10.
OPM-12	OPM-FIS	Tammy Paul (Operational Policy)			391-393		There are different sources for the records of a background investigation such as the OPF, the eOPF, and CVS. Recommend using the term "record" in the statement since it has to be contained in a system of records.	Ensure language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Resolved by replacing: This collection is not necessary for applicants who have a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation that can be located and referenced. with: This collection is not necessary for applicants who have a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation on record that can be located and referenced.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OPM-13	OPM-FIS	Tammy Paul (Operational Policy)	Technical		448-449		Should the results of the investigation be on the card? I think this is improper. It is more approriate to have the status of the investigative results on the card or else the final determination on the card. It is too risky to have the investigatve results themselves located on the card.	Text should reflect that investigative results should not be on the credential.	Declined. The referenced text recommends that the current status of the background investigation be included in the chain-of-trust, not on the card; however, it is noted that this comment concerns the protection of sensitive and Personally Identifiable Information. Credentials and Identity Management Systems must protect data as directed under laws and directives such as the Privacy Act and HSPD-12.
OPM-14	OPM-FIS	Tammy Paul (Operational Policy)	General	9	482-487	2.7	The ARC has not yet been defined. In the draft FIS standards, it is a process, not a set of particular checks. This is a similar issue to the NAC check, which is also not an investigation. Its use is inconsistent with the Springer Memo for determinations for interim and final PIV credentials.	Suggest removal of text on the ARC until the draft federal investigative standards have been finalized. Ensure language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Resolved by using the term "NAC" instead of "ARC" throughout the document. On first occurrence of the term "Nation Agency Check (NAC)", insert the following footnote: The NAC is an automated record check.
OPM-15	OPM-FIS	Tammy Paul (Operational Policy)	Technical	10	533 - 537		**Is this consistent with the Springer memo?**	Ensure policy and language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Noted. This section describes identity proofing and registration only. The Springer memo covers investigative requirements.
OPM-16	OPM-FIS	Tammy Paul (Operational Policy)	general	11	482-487 and 549-552	Section 2.8	FIPS 201 does not have authority to provide the investigative and adjudicative processes for physical and logical access to federal facilities and information systems. As the Suitability Executive Agent under EO 13467, OPM is the authority which develops and implements uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability and eligibility for logical and physical access to federally controlled facilities or information systems.	Delete lines 485-487 and 549-552. Ensure policy and language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Declined: The requirements are consistent with M-05-24 and the federal investigative standards. See also OPM-6.
OPM-17	OPM-FIS	Tammy Paul (Operational Policy)	General	11	546-552	2.8	The ARC has not yet been defined. In the draft FIS standards, it is a process, not a set of particular checks. This is a similar issue to the NAC check, which is also not an investigation. Its use is inconsistent with the Springer Memo for determinations for interim and final PIV credentials.	Suggest removal of all text on the ARC until the draft Federal Investigative Standards have been finalized. Ensure language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Resolved by OPM-14.
OPM-18	OPM-FIS	Tammy Paul (Operational Policy)	General	11	552		*The PIV Card shall be revoked if the results of the background investigation so justify*. There is risk here to federal facilities and systems. It's possible that an individual was given logical/physical access prematurely based on the FBFP name. The card would not be revoked until completion of the full investigation & adjudication. To bolster this argument, note the concern in this document over a period of 18 hours. (Line 680, page 14). Full investigation & adjudication may take weeks as opposed to 18 hours.		Noted.
OPM-19	OPM-FIS	Tammy Paul (Operational Policy)			582-598		*Is the grace period going to be consistent with the new Federal Investigative Standards? Is "valid" the correct term?*	Ensure policy and language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Noted. As per discussion with OPM, the grace period does not conflict with the new federal investigative standards. See also OPM-28.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OPM-20	OPM-FIS	Tammy Paul (Operational Policy)	Technical	12	617		*The issuer shall verify that the employee's or contractor's background investigation is **valid** before…* The term "valid" is imprecise. Suggest "reciprocal" to align with OPM terminology and policies.	replace "valid" with "reciprocal."	Resolved by using the word 'valid' throughout the document, as discussed with OPM, since the the word 'current' or 'reciprocal' could lead to misinterpretations.
OPM-21	OPM-FIS	Tammy Paul (Operational Policy)	General	13	633-634		I am confused over the 6 year validation requirement: (line 568) *The PIV Card shall be valid for no more than six years. (Line 633-634) Previously collected biometric data may be reused with the new PIV Card if the expiration date of the new PIV Card is no later than 12 years after the date that the biometric data was obtained.* Does this mean that prints will be repeated every 12 years, but cards will be issued every 6. Thus new prints are captured every other time?	Ensure policy and language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Noted. The requirements as specified would allow an issuer to collect new biometric data every other time that a PIV Card is issued. This requirement is related to biometric data that is stored on the PIV Card (as described in Section 4.2.3.1) and is not tied to background investigation.
OPM-22	OPM-FIS	Tammy Paul (Operational Policy)	Technical	13	661		*"valid"* (same comment as above).	Suggest "reciprocal" or "current".	Per discussion with OPM, the terms "current" and "reciprocal" are inappropriate in this context. See also OPM-20.
OPM-23							MISSING		Noted.
OPM-24	OPM-FIS	Tammy Paul (Operational Policy)	general			2.9.5	OPM's standards provide information on when a card should be issued or revoked.	Add relevant circumstances to ensure policy and language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Noted per discussion with OPM.
OPM-25	OPM-FIS	Tammy Paul (Operational Policy)	Technical	16	754		*a cardholder is determined to hold a fraudulent identity; or* This is an adverse situation, where the others in the list are benign. Suggest this be re-categorized as a "revocation." (AKA, the definition, "terminated with cause.")		Resolved by listing "a cardholder is determined to hold a fraudulent identity;" as the last bullet of the list.
OPM-26	OPM-FIS	Tammy Paul (Operational Policy)	General			Section 2.8	I think "on record" may need to be clarified. Agencies may still have the investigation in their security file but the ISP may no longer have it on record. Perhaps it would be better to require that the investigation still be on record with the Investigation Service Provider and/or on record in the Central Verification System (CVS).		Noted. Additional information is available in FAQ #15 in http://www.idmanagement.gov/documents/hspd12_faqs_policy.pdf.
OPM-27							MISSING		Noted.
OPM-28	OPM-FIS	Tammy Paul (Operational Policy)				Section 2.8	This section does not list a grace period for break in service but lists it to be a brief lapse. I'd recommend adding that the lapse could not exceed 2 years. This aligns with the requirement to conduct a new investigation when there has been a break in service of greater than 2 years. However, this could change when upon finalization of the Federal Investigative Standards. Additionally in this section, it indicates that the background investigation must be "valid". I'd recommend adding some clarification to what "valid" means. Likely it means that a previously completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation is on record with the Investigation Service Provider and/or on record in the Central Verification System (CVS).	Ensure language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications and with the revised Federal Investigative Standards.	Resolved by adding a footnote to the end of the first paragraph as follows: "For the purposes of this section, a lapse is considered to be brief if it is not long enough to require that a new background investigation be performed. OPM currently requires a new background investigation to be performed when there has been a break in service of greater than two years."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OPM-29	OPM-FIS	Tammy Paul (Operational Policy)			2050-2051		FIPS-201 and the Springer Memo need to cross reference one another. The lack of a definition of an IDMS system is problematic.	Reinsert definition of an Identity Management System and add relevant text.	Resolved by adding the following definition: Identity Management System -- Identity management system comprised of one or more systems or applications that manages the identity verification, validation, and issuance process.
OPM-30	OPM-FIS	Tammy Paul (Operational Policy)			2127		The ARC has not been defined in the Federal Investigative Standards	recommend removing reference to the ARC until FIS is finalized.	Resolved by OPM-14.
OPM-31	OPM-FIS	Tammy Paul (Operational Policy)	General				OPM is undergoing special review of policies and procedures regarding the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability and eligibility for logical and physical access in order to ensure uniformity and consistency with the Joint Reform Effort and the new the Federal Investigative Standards. Recommend extensive dialogue with OPM to ensure consistency with FIPS-201.	Ensure language is current, coordinated and consistent with OPM's policies on credential investigations and adjudications.	Noted. NIST engaged in extensive dialog during the development of Revised Draft FIPS 201-2, and will do so again, as necessary, when addressing relevant comments submitted on the Revised Draft.
ORC-1	Operational Research Consultants, Inc.	Benjamin Brown		28	1075	4.1.4.1	Are there restrictions on the terms used for Zone 8F, Employee Affiliation? Do the examples presented originate from any particular source or standard?		Noted. The description for Zone 8F does not impose any restrictions on the terms that may be used in that zone. "Employee," "Contractor," "Active Duty," and "Civilian," are specifically listed as examples.
ORC-2	Operational Research Consultants, Inc.	Benjamin Brown		9	491	2.7	If an individual presents two (2) valid forms of ID, one bearing the name "Terrence William Smith" and the other "T. William Smith", would the Registrar be obligated to ask for another form of ID matching either of the names?		The July 2012 Draft FIPS 201-2 states that "If the two identity source documents bear different names, evidence of a formal name change shall be provided." In the presented scenario, both identity source documents bear the same name, and so there would be no requirement for the cardholder to present evidence of a formal name change or to present a third form of ID.
ORC-3	Operational Research Consultants, Inc.	Benjamin Brown		27	1070	4.1.4.1	If an individual presents two (2) valid forms of ID bearing the name "T. William Smith", can the card be printed with just "T. W. Smith"?		Line 1070 in the July 2012 Draft FIPS 201-2 states that "Names in the Primary Identifier and the first name in the Secondary Identifier shall not be abbreviated." Thus, the first name in the Secondary Identifier cannot be abbreviated.
OSE-1	Open Security Exchange	Ron Martin	G				HSPD-12 and the subsequent FIPS 201 have went to great length to establish accurate Identities. This revision must establish protocols to forensically analyze breeder document to assure the document is consistent with the issuer's design characteristics.	Recommend that the reviewers determine the best of breed of these document authenticator devices to assure that the PIV Cards are "NOT" issued as the result of CALIBRATED EYEBALLS.	Resolved by AT-2.
OSE-2	Open Security Exchange	Ron Martin	T	vii	194-197	10	Here the text is requiring mandatory "Card Features". To clarify this requirement a further description is needed. The CAK is a required Data Object.	Insert after the word "Features" the phrase "data objects"	Declined. The term 'Feature' is sufficient because it describes data objects as well as other capabilities such as secure messaging, authentication methods (e.g., OCC-AUTH) etc.
OSE-3	Open Security Exchange	Ron Martin	E	vii	202-205	10	The FICAM Version 2 was issued after the first draft of FIPS 201-2. Therefore, the present tense should be used.	On line 203 delete "will be" Replace with "is" also, add to the end of line 205 as follows: …" guidance, version 2."	Declined. The use of future tense is appropriate to indicate the need to update the Roadmap in order to align with FIPS 201-2.
OSE-4	Open Security Exchange	Ron Martin	T	viii	210-211	11	This is a false assumption. With the prevalence of false credentials such as False PIV Cards, Driver's Licenses and Passports this cannot be assured. If a person purchase or produce a fraudulent PIV Card this statement is false. If the credential identity is based on personal observation of the breeder document the human cannot read 2D bar codes/magnetic stripes to compare the ID information to printed on the card.	Delete the words at the end of line 211 "…correctly Identified.." Replace with "..correctly Identity Proofed…"	Declined. Identity proofing is the means by which the issuer can provide assurance "that the individual in possession of the credential has been correctly identified."
OSE-5	Open Security Exchange	Ron Martin	T	1	203	1	How is the " Authentication of an individual's Identity performed? There is nothing in the current document that require Breeder Document Authentication/Verification to obtain the credentials to allow logical and physical access.	Re-write this paragraph at such time that responsible authentication methods are prescribed.	Resolved by OPM-3 and AT-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OSE-6	Open Security Exchange	Ron Martin	T	1	239	1	IBID Comment	IBID Comment	Resolved by OPM-3.
OSE-7	Open Security Exchange	Ron Martin	E	4	323-325	1.4	Section 2 is normative. However, 2.6 is informative. (Optional) So that there would not be any confusion a description here should explain the directive/optional portions.	As appropriate, state that within the normatively referenced section there are optional subsections. Optional references will be identified with informative language.	Declined. Optional is not the same as informative. For example, it is optional to collect and store iris images on PIV Cards, however, the text describing the collection and storage of this data is normative, since it must be followed by those that choose to collect and store iris images on PIV Cards.
OSE-8	Open Security Exchange	Ron Martin	G	7	431	2.6	The Phase "Chain of Trust" is used in over 30 instances. At least 10 instances the term is used differently.	The standard need to outline the different applications of the term	Declined. The term "chain-of-trust" is used consistently throughout the document.
OSE-9	Open Security Exchange	Ron Martin	T	7	431-433	2.6	Although the chain of trust is optional, the card issuer must be assured that the person presenting him/herself is indeed the person sponsored.	Add after the word "collects" line 433: Therefore, the chain of trust begin with a true electronically verified breeder document. All identification such as name, date of birth and other personal information must match the sponsor entered information.	Declined. The suggested text is related to identity proofing, not the maintenance of a chain-of-trust.
OSE-10	Open Security Exchange	Ron Martin	T	7	437-438	2.6	The device performing the breeder document verification can log the date, time, location, name and title of the breeder document.	add after the word "collected" on line 438: during the electronic breeder document verification, the card issuer should log the date, time, location, name and title of the breeder document from the verifying device. No PII should be retained by this process.	Resolved by OSE-9.
OSE-11	Open Security Exchange	Ron Martin	T	41130	476/489/490	2.7	Section 2.7 Identity Proofing is a normative requirement. I reference a 2004 white paper presented to the IEEE Conference on technologies for Homeland Security authored by Theodore Kuklinski, PhD. http://www.advancediddetection.com/uploads/1/0/5/6/10560305/automated_authentication_of_current_identity_documents.pdf In 1998 100,000 fraudulent were intercepted at US ports. Current ID Chief from China has a large following in the United States Citizens acquiring fraudulent ID Cards. This Fakes are difficult to detect with the naked eye. Finally, if an applicant knowingly present a fraudulent Breeder document that applicant should be referred to the cognizant law enforcement authority. Under Title 18 of the United States Code.	Add the following after the word "form" on line 490: All Identity source documents shall be electronically verified and authenticated as a document consistent with the credential issuer's design characteristics including security features. If a source document is presented to the identity proofing registered agent and/or other official representative of the government and it is found to be suspect as a fraudulent government document the agency will confiscate the document and refer the applicant to the cognizant Law Enforcement Authority for further investigation under Chapter 47 of Title 18 of the United States Code (USC) Fraud and False Statements, see http://uscode.house.gov/download/pls/18C47.txt	Resolved by AT-13.
OSE-12	Open Security Exchange	Ron Martin	T	41	1265	4.2.1	If the CHUID will be removed in five years, why include it?	Remove the section. In other words be silent on the CHUID	Declined. As stated in Appendix E - the Revision History: "The CHUID data element has not been deprecated and continues to be mandatory." Section 6.2.5 states that it is expected that the CHUID authentication mechanism will be removed at the next five-year revision, not the data element.
OSE-13	Open Security Exchange	Ron Martin	E	42	1274	4.2.1	The text uses CMS as Cryptographic Message Syntax. Common use of the term Is Card Management System	Recommend CMS usage be standardized .	Noted. As is the case with many acronyms, CMS has more than one use, and it is also commonly used to mean Cryptographic Message Syntax. In FIPS 201-2, CMS is only used to mean Cryptographic Message Syntax, and Card Management System is always spelled out.
OSE-14	Open Security Exchange	Ron Martin	E	59-60	1834-1850		OMB M 11-11 require PIV Enablement.	Change line 1834 from "Should Be" to "will" Change Line 1850 from "May be" to "Will"	Declined. Both lines 1834 and 1850 say "The PIV Card may be used," which is an accurate statement. (Line 1834 does not say "should be"). The use of the term "will be" would be incorrect without appropriate qualifying statements.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OT-1	Oberthur	C. Goyet	G				FIPS 201-2 relies on SP800-73 and SP800-76 to provide technical details on the new features like secure messaging and OCC. So FIPS 201-2 cannot become effective before SP800-73 is updated and NPIVP cannot validate product compliance with SP800-73 before SP800-85 is released and assocaited test tool is developped. To minimize the delay after FIPS 201-2 publication and before the first compliant produt can be listed on the GSA APL, could NIST release SP800-73-4 as they did for SP800-76-2 as draft for public comments so this can be reviewed together with FIPS 201-2?	Release for public comments SP800-73-4 that provides implementation details for the new features introduced by FIPS 201-2 like secure messaging and OCC, so that SP can be reviewed together with draft SP800-76-2 and FIPS 201-2 already published for public comments.	Resolved by DHS TWIC-1.
OT-2	Oberthur	C. Goyet	T	6	402		Using the same fingerprints for on-card and off-card comparison introduces a significant security flaw, and defeats the purpose of the CHANGE PIN functionality. Indeed anyone who has a temporary access to an activated card, (or to a card and its PIN), would be able to dump from the card the template for off-card comparison and retrieve from it the template for OCC using the method described in SP800-76-2 second draft. Even if the legitimate card holder finds out that his PIN was compromised, he may define a new PIN using the CHANGE PIN function, but the hacker would still be able to activate the card and perform any PIN protected operation like signature, using the OCC template. Unlike PIN, Fingerprint cannot be changed and a one time access to off-card comparison template provides a lifetime access to all PIN protected card operations. Since the OCC provides the same rights as PIN verification, the OCC template should be considered as a permanent activation key and be provided a higer level of protection than PIN protected PIV data. That is why it is important that templates for OCC cannot be derived from less secure templates for Off card comparison. There are at least two ways to acheive this. The frist one is to use different fingers for off-card and on-card fingerprint verification, but this could be confusing to the card holder. The alternative is to disable off-card comparison on cards fitted with on-card comparison.This could be acheived by removing the PIV fingerprint container when on-card comparison has been activated (or at least erasing its content).	Change the sentence to: Two fingerprints, for on-card comparison, **which are preferably not** the same as the two fingerprints collected for off-card comparison, and make the PIV fingerprint container optional so both off-card and on-card verification cannot be performed with the same card.	Resolved by AMAG-5.
OT-3	Oberthur	C. Goyet	T	7	429		Can the facial image be used for automated facial recognition software ?	Clarify whether facial image that is now mandatory can be used with matching algorithms like other PIV biometrics can.	Resolved by AMAG-6 and by revising the sentence "may be used for biometric authentication in operator-attended PIV issuance, reissuance, renewal and verification data reset processes." to "may be used for automated facial authentication in operator-attended PIV issuance, reissuance, and verification data reset processes."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OT-4	Oberthur	C. Goyet	T	24	957		ISO/IEC 10373 does not define card physical characteristics but test methods to assess card compliance with ISO/IEC 7810, 7816, 14443 etc…	Change the sentence to : The PIV Card shall comply with physical characteristics as described in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], , ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards [ISO14443] using test methods defined in ISO/IEC 10373 [ISO10373].	Declined. Although ISO/IEC 10373 is a conformance testing standard, it becomes the basis for the durability requirements for the PIV card material.
OT-5	Oberthur	C. Goyet	T	27	1065		"The font size 7 point allows space for 3 lines and shall only be used if the full name is greater than 45 characters. " Actually what is important is not as much the number of characters than the number of "W" vs "I" type of letters present in the name.	replace the sentence with "The font size 7 point allows space for 3 lines and shall only be used if the name does not fit on two lines with font 8."	Resolved by DHS TWIC-5.
OT-6	Oberthur	C. Goyet	T	28	1073		What should be the criteria used by the printer to decide whether to print SMITH-JONES, SUSIE MARGARET versus SMITH-JONES, SUSIE MA> RGARET ? One way to solve that issue is to ask the card holder define during enrollement what part oh the name should be on each 3 lines and have a software to compute the actual space needed depending on the letters used to validate the card holder choice.	Add a sentence that the way the name is be printed should be defined by the card holder during enrollment.	Resolved by DHS TWIC-6.
OT-7	Oberthur	C. Goyet	T	35	1202		Could you please define more precisely the Tactile markers to be used in zones 21F and 22F? Are there any standard they should comply with? Can they be freely picked? What validation testing would ensure the effectiveness of these markers?	Provide technical specifications or reference to a standard to define the tactile markers that are acceptable for zone 21F and 22F and validation procedure.	Resolved by DHS TWIC-7.
OT-8	Oberthur	C. Goyet	T	42	1293		Could a symmetric key be used as well to establish the secure messaging like Global Platform SCP03?	Change the sentence to : The PIV Card may include **a symmetric** or an asymmetric private key and corresponding public key certificate to establish symmetric keys for use with secure messaging,	Resolved by DHS TWIC-15.
OT-9	Oberthur	C. Goyet	T	44	1389		Can the PIV card application administration key be used over the virtual contact?	change the sentence with: If present, the cryptographic operations that use the PIV Card Application Administration Key must only be accessible using the contact **or virtual contact** interface of the PIV Card.	Resolved by DHS TWIC-16.
OT-10	Oberthur	C. Goyet	T	55	1689		Authentication Using On-Card Biometric Comparison (OCC-AUTH): The response includes information that allows the reader to authenticate the card. According to ISO/IEC 7816-4 the Verify command shall not return any data besides the two byte status word so no authentication data can be returned at this time. However it is stated earlier in the document that a successful OCC_AUTH can be used to activate the PIV card, therefore to unlock the PIV Authentication key allowing the authentication to proceed as if the PIN was verified. But this has to be a two step process.	replace "The response includes information that allows the reader to authenticate the card. " with "a successful OCC activate the PIV card and allows authentication with the PIV authentication key.	Resolved by DHS TWIC-22.
OT-11	Oberthur	C. Goyet	T	57	1752		A unique identifier within the data element is used as input to the authorization check to determine whether the cardholder should be granted access. Since the data element is no longer always the CHUID but could now be also from an authentication certificate, how does the reader know which data element to use?	Specify which unique identifier to return or replace sentence with : The UUID from the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access.	Resolved by DHS TWIC-23.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OT-12		C. Goyet			1196	Figure 4-2		I've noticed that the specific font size for zone 12F was added in SP800-104 (Arial 7pt bold) when no specific font was provided in FIPS 201-1 for that zone. By increasing the font to 7pt, SP800-104 had to remove the word "Federal" to fit in the banner, so only "Emergency Response Official" is printed. But FIPS 201-2 reintroduces the word "Federal" and remove the specific font information for zone 12, making it the default font of 6pt bold.	Resolved by withdrawing SP 800-104. Zone 12F, therefore, will default to 6 pt bold Arial and include the word 'Federal'. The font used in figure 4-2 will be resized accordingly.
PB-1	Precise Biometrics	Michael Harris	G	vi	142	6	Biometric authentication off-card in risk areas is not recommended and is opposed. When and if the head of a department desires to employ biometrics the usage of such should be limited to OCC (On Card Comparison) so that the sensitive templates and processing are not exposed.	...wireless and/or off card biometric capabilities...	Declined. The text already says "the head of a department or independent agency may issue a select number of maximum security credentials that do not contain (or otherwise do not fully support) the wireless and/or biometric capabilities otherwise required/referenced herein." Changing "biometric capabilities" to "off card biometric capabilities" would be confusing since it could be interpreted to mean that such cards would be required to support on-card biometric comparison, whereas support for OCC is optional.
PB-2	Precise Biometrics	Michael Harris	T	vii	198 and 199	10	Line 190 states the standard is to be made effective immediately. Line 196 indicates all new or replacements cards must comply 'no later than' 12 months from the effective date. Line 198 and 199 allows for accrediation of PIV issuers to be in compliance 12 months 'after' the effective date. This is temporally incongruous	Propose that PIV issuers accredited at or after the effective date must be in compliance. This allows agencies a potential maximum of 12 months to issue new and replacement cards per the intent of the specification.	Declined. Issuers need to be given time to come into compliance with the new requirements. The proposed change would require issuers whose accreditations are due shortly after the effective date for FIPS 201-2 to have to come into compliance with the new requirements almost immediately.
PB-3	Precise Biometrics	Michael Harris	G	viii	223	11	The standard intent is to provide high assurance identity verification with appropriate levels of security and assurance. Lines 221-223 correctly state that system behavior is a discrete entity from individual or composite functional elements. While system functionality in reference to security is explicitly stated the section does not express the need for validation of system level functional integrity.	Propose: …overall system provides the acceptable level of security and functional integrity to ensure end state compliance.	Declined. Functional integrity is an inherent part of security. Validation is a means of ensuring that an acceptable level of security has been achieved.
PB-4	Precise Biometrics	Michael Harris	G	VIII	225	11	Moores law and the state of technology advancement today tends to indicate a series of technical evolutions would yield revolutionary alterations in less than 5 year periods. It is also relevant to note that review, revision and implementation draws out the period of new implementation by an additional 16-30 months.	…review this Standard within 3 years…	Declined. It is common for FIPS to be reviewed within 5 years of publication and a review of this Standard. See also DoD-2 and SSA-1. Also note that many of the details of PIV have been placed in Special Publications, which allows them to be updated prior to the next revision of FIPS 201 itself.
PB-5	Precise Biometrics	Michael Harris	E	1	204	1	FIPS covers physical and logical assets and should be extended beyond "computer systems, or data"	…buildings, data, or digital processing systems (including but not limited to, computer systems, mobile platforms,etc.)	Declined. We believe that the term "computer systems" will be more easily understood than "digital processing systems," and see no reason why "computer systems" would be considered to be a subset of "digital processing systems."
PB-6	Precise Biometrics	Michael Harris	E	1	210	1	Reference to computers and data is limiting and does not extend to the full intent of the Standard. Mobile phones and tablets may have processing capabilities but not be considered "computers" Suggest expanding this to a more universal terminology.	…authorization to data and data processing platforms… (or) …authorization to data and digital and data processing products	Resolved by PB-5.
PB-7	Precise Biometrics	Michael Harris	E	1	228	1	Federal government-wide' may be considered redundant	propose: "…identifies Federal requirements..."	Declined. The statement is referring to requirements that apply across the Federal government (i.e., "-wide" is a qualifier for "Federal government"), so it is not redundant.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
PB-8	Precise Biometrics	Michael Harris	E	6	402	2.4	Two fingerprints collected for On-Card may be physically the same as the two fingerprints collected for off-Card, however, they are syntactically different data representations.	Suggest foot note: The on-card and off-card fingerprint reference data are stored separately and, as conformant instances of different formal fingerprint standards, are syntactically different. This is described more fully in [SP 800-76].	Declined. Section 2.4 is about the collection of biometric data, whereas the suggested footnote (which already appears in Section 4.2.3.1) is about the representation of the representation of the data on the card. The footnote does not belong to Section 2.4 but it properly belongs in Section 4.2.3.1.
PB-9	Precise Biometrics	Michael Harris	T	8	467	2.6	Operator assisted authentication and reissuance is required with biometric enrollment data for corellation to the chain-of-trust. The card issuer should validate/perform the cardholder 1:1 biometric match.	Propose: "…the card issuer shall perform a 1:1 biometric match of the cardholder to reconnect to the card issuer's chain-of-trust."	Declined. The verb 'can' is used to indicate that CoT is optional to implement and that there alternatives to 1:1 biometric match in cases where the biometric match failed -- as described in section 2.9.1 Note: If the issuer does not implement the CoT, the the entire Identity Proofing and Registration Process is repeated as per section 2.9.1.
PB-10	Precise Biometrics	Michael Harris	T	21	873	3.1.1	Disambiguation requested for footnote (10) and lines 879-880. "Alternatively, on-card biometric comparison can be used to activate the PIV card" v. "…use of biometrics provides an additional factor of authentication"	Propose:"In addition to the use of On Card Comparison for card activation, the use of biometrics provides an additional factor of authentication…"	Declined. The paragraph is specific to PIN input devices and card activation. Section 3.1.1 last paragraph discusses biometric input device and Section 6.2.1 discusses OCC in detail.
PB-11	Precise Biometrics	Michael Harris	E	45	1405	4.2.3.2	Suggest addition of text for improved clarity and comprehension when specifying CBEFF headers as required for all biometric records intended for off card comparison.	Propose: "The biometric records designated for off-card comparison shall be prepended…"	Declined. The proposed text would likely create confusion rather than improving clarify. The CBEFF headers are required for all biometric data, except for the fingerprint templates for on-card comparison. The proposed additional text ("designated for off-card comparison") could be incorrectly interpreted to mean that the CBEFF header is only required for biometric data that the issuing agency intends to use for off-card comparison.
PB-12	Precise Biometrics	Michael Harris	G	47	1476	4.4.1	Discussion of contact readers is made in reference to physical access control systems and general desktop computing systems for logical access.	The standard should be broadened to include other contgrolled data processing platforms (e.g., special purpose control systems, mobile data systems, etc.)	Resolved by deleting "physical access control" from the final sentence of Section 4.4.1.
PB-13	Precise Biometrics	Michael Harris	G	47	1483	4.4.2	Discussion of contact readers is made in reference to physical access control systems and general desktop computing systems for logical access.	The standard should be broadened to include other contgrolled data processing platforms (e.g., special purpose control systems, mobile data systems, etc.)	Resolved by deleting "physical access control" from the fourth sentence of Section 4.4.2 and deleting the final sentence of Section 4.4.2.
PB-14	Precise Biometrics	Michael Harris	T	48	1501	4.4.4	When using OCC or PIN for logical access, the input device is not required for integration with the PIV card reader. This introduces several potentials for threat vectors.	Require OCC and PIN input devices for logical access to be integrated with the PIV reader or further specify "transmitted securely and directly" in the context of section 4.4.4. SP 800-76 defines the technical functions but not the implementation as a system for secure transmission and processing.	Resolved by DoD-55 from the disposition of comments on the March 2011 FIPS 201 Draft.
PB-15	Precise Biometrics	Michael Harris	T	54	1667	6.2.1.1	The Standard specifies that OCC or PIN may be used for card activation. Line 1667 specifies only the PIN. Since the template data is unique and different, either PIN or OCC should be viable for card activation in this context	Propose: "…to submit a PIN or OCC match, activating the PIV card."	Declined. As stated in Section 4.2.3.3, biometric data may only be read from the card if the card has been activation using PIN-based authentication. OCC may be used to activate the PIV Card to perform private key operations, but not to read the biometric data from the card.
PB-16	Precise Biometrics	Michael Harris	G	60	1857	6.3.2	Since CHUID provides little or no confidence of identity it is not appropriate to specify local or network access with this mechanism	Remove the option for CHUID as a logical access authentication mechanism	Declined. As noted in Section 6.2.5, the use of the CHUID authentication mechanism is deprecated and may be removed in the next revision of the Standard. As the CHUID authentication mechanism is permitted for authentication to a local workstation environment in FIPS 201-1, it would be inappropriate to entirely remove it as an option in FIPS 201-2.
PB-17	Precise Biometrics	Ramon Reyes	E	iii	65	ABSTRACT	The term electronic access is only referenced in this section. Should be replaced by logical access.	Propose: …to Federally controlled government facilities and logical access to government information	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
PB-18	Precise Biometrics	Ramon Reyes	T	15	721	2.9.4	The proliferation and general use of smart-card enabled mobile devices should enable unattended PIN reset.	Propose: Pin reset at an unattended issuer-operated kiosk or thru a smartcard reading enabled mobile device shall ensure that the cardholder's biometric matches…"	Declined. The proposed text would seem to suggest that the requirements specified for issuer-operated kiosks could also apply to any smart-card enabled mobile devices, even ones that are not issuer-operated. PIN resets performed using devices that are not issuer-operated would have to follow the requirements for remote reset.
PB-19	Precise Biometrics	Ramon Reyes	T	46	1426	4.2.3.3	On-card biometric comparison can be used to enable PiV Card Verification Data Reset	On-card biometric comparison may be performed over the contact and the contactless interfaces of the PIV Card to support card activation (Section 4.3.1), PIV Card Verification Data Reset (2.9.4) and cardholder authentication (Section 6.2.2)	Declined. In the case of PIN resets, on-card biometric comparison is used to authenticate the cardholder as one step in the reset process. The PIN cannot be directly reset as a result of an on-card biometric comparison operation.
SCA-1	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	T	2	260	1.3.1	A backward compatible change is a change or modification to an existing feature that does not break the systems using this feature. For example, changing the Card Authentication certificate from optional to mandatory does not affect the systems using the Card Authentication certificate for authentication (i.e., using the PKI-CAK mechanism).	Relying system components deployed by organizations who choose to not implement this optional function may not support this option and may require update	Noted. Mandating that a feature appear on the card is not the same as requiring relying system components to be able to make use of this feature. So, the implication that relying systems that do not make use of the previously optional feature would "require update" is not accurate.
SCA-2	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	T	2	265	1.3.2	A non-backward compatible change is a change or modification to an existing feature such that the modified feature cannot be used with existing systems. For example, changing the format of the biometric data would not be compatible with the existing system, because a biometric authentication attempt with the modified format would fail. Similarly, changing the PIV Card Application IDentifier (AID) would introduce a non-backward compatible change. As a result, all systems interacting with the PIV Card would need to be changed to accept the new PIV AID.	Relying system components deployed prior to the additional AID being defined may require update to recognize additional AIDs.	Noted. This is already covered by the statement that "all systems interacting with the PIV Card would need to be changed to accept the new PIV AID."
SCA-3	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	T	2	272	1.3.3	New features are optional or mandatory features that are added to the Standard. New features do not interfere with backward compatibility because they are not part of the existing systems.	New features may interfere with backward compatibility because they are not part of the existing systems.	Declined. New features of a card are not yet implemented by the relying system, and therefore, no backwards compatibility problem can exist.
SCA-4	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	T	41	1272	4.2	The CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card without card activation.	The CHUID may be accessible from either the contact or, after a virtual contact interface is established, the contactless inteface	Declined. The CHUID is available for free-read over both the contact and the contactless interface. There is no requirement to establish a virtual contact interface to read the CHUID over the contactless interface.
SCA-5	Smart Card Alliance	Walter Hamilton, ID Technology Partners/ Roger Roehr, Roehr Consulting	T	46	1424	4.2.3.3	This states that biometric data stored on the card may optionally be readable through the virtual contact interface after presentation of a valid PIN. FIPS 201-2 further states that the virtual contact interface will be defined in SP 800-73. It would be preferable to not restrict the ability to read the biometric over the virtual contact interface without a PIN as long as a trusted communciation session between the card and the reader has been established. While the next revision to SP 800-73 may or may not define a mechanism where the card can trust the reader, it is conceivable that such a capability could be added to SP 800-73 prior to the next five year cycle review of FIPS 201.	Change line 1424 and 1425 to read as follows: "…may optionally be readable through the virtual contact interface and after the presentation of a PIN. A PIN is not required if the communication session established between the card and the reader provides for a capability to ensure that the reader can be trusted by the card in a manner that is in accordance with [SP 800-73]."	Resolved by DHS TWIC-18.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-6	Smart Card Alliance	Christophe Goyet, Oberthur	G				FIPS 201-2 relies on SP800-73 and SP800-76 to provide technical details on the new features like OCC. So FIPS 201-2 cannot become effective before SP800-73 and SP800-76 are updated and NPIVP cannot validate product compliance with SP800-73 before SP800-85 is released and associated test tool is developed. To minimize the delay after FIPS 201-2 publication and before the first compliant products are listed on the GSA APL, could these Special Publications be released as draft for public comments simultaneously with FIPS 201-2 and could the NPIVP validation tool be developed simultanously with SP800-85?	Release for public comments ASAP all of the Special Publications that would be needed to develop and validate compliance with FIPS 201-2 to shorten the development cycle for manufacturers so FIPS 201-2 compliant products can be acquired by Federal agencies reasonably quickly after FIPS 201-2 publication.	Resolved by DHS TWIC-1.
SCA-7	Smart Card Alliance	Christophe Goyet, Oberthur	T	7	429	2.5.	Can the facial image be used for automated facial recognition software ?	Clarify whether the facial image that is now mandatory can be used with matching algorithms like other PIV biometrics can.	Resolved by OT-3.
SCA-8	Smart Card Alliance	Christophe Goyet, Oberthur	T	27	1065	4.1.4.1	"The font size 7 point allows space for 3 lines and shall only be used if the full name is greater than 45 characters. " Actually what is important is not as much the number of characters than the number of "W" vs "I" types of letters present in the name.	Replace the sentence with "The font size 7 point allows space for 3 lines and shall only be used if the name does not fit on two lines with font 8."	Resolved by DHS TWIC-5.
SCA-9	Smart Card Alliance	Christophe Goyet, Oberthur	T	28	1073	Table 4-1	What should be the criteria used by the printer to decide whether to print SMITH-JONES, SUSIE MARGARET versus SMITH-JONES, SUSIE MA> RGARET ? One way to solve that issue is to ask the cardholder to define during enrollement what part of the name should be on each of the 3 lines and have software compute the actual space needed depending on the letters used to validate the cardholder choice.	Add a sentence that the way the name is be printed should be defined by the cardholder during enrollment.	Resolved by DHS TWIC-6.
SCA-10	Smart Card Alliance	Christophe Goyet, Oberthur	T	35	1202	4.1.4.4	Could you please define more precisely the Tactile markers to be used in zones 21F and 22F? Are there any standard they should comply with? Can they be freely picked? What validation testing would ensure the effectiveness of these markers?	Provide technical specifications or reference to a standard to define the tactile markers that are acceptable for zones 21F and 22F and validation procedure.	Resolved by DHS TWIC-7.
SCA-11	Smart Card Alliance	Christophe Goyet, Oberthur	T	42	1293	4.2.2	Could a symmetric key be used as well to establish the secure messaging -- like Global Platform SCP03?	Change the sentence to: The PIV Card may include a symmetric key or an asymmetric private key and corresponding public key certificate to establish symmetric keys for use with secure messaging,	Resolved by DHS TWIC-15.
SCA-12	Smart Card Alliance	Christophe Goyet, Oberthur	T	44	1389	4.2.2	Can the PIV card application administration key be used over the virtual contact?	Change the sentence with: If present, the cryptographic operations that use the PIV Card Application Administration Key must only be accessible using the contact or virtual contact interface of the PIV Card.	Resolved by DHS TWIC-16.
SCA-13	Smart Card Alliance	Christophe Goyet, Oberthur	T	55	1689	6.2.2	Authentication Using On-Card Biometric Comparison (OCC-AUTH): The response includes information that allows the reader to authenticate the card. According to ISO/IEC 7816-4 the Verify command shall not return any data besides the two byte status word so no authentication data can be returned at this time. However it is stated earlier in the document that a successful OCC_AUTH can be used to activate the PIV card, therefore to unlock the PIV Authentication key allowing the authentication to proceed as if the PIN was verified. But this has to be a two step process.	Replace "The response includes information that allows the reader to authenticate the card. " with "A successful OCC activates the PIV card and allows authentication with the PIV authentication key.	Resolved by DHS TWIC-22.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-14	Smart Card Alliance	Christophe Goyet, Oberthur	T	57	1752	6.2.4	A unique identifier within the data element is used as input to the authorization check to determine whether the cardholder should be granted access. Since the data element is no longer always the CHUID but could now be also from an authentication certificate, how does the reader know which data element to use?	Specify which unique identifier to return or replace sentence with : The UUID from the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access.	Resolved by DHS TWIC-23.
SCA-15	Smart Card Alliance	Roger Roehr, Roehr Consulting	T	38	1188	4.1.4.4	Make the GUID in the CHUID a mandatory data element. At this time the GUID is not mandatory for Federal issuers and requires systems to do a discovery to see if the credential is a PIV or PIV-I, and then use FASC-N for federal issuers and GUID for PIV-I issuers. This would unify the credential process.	4.2.3 GUID This standard requires the inclusion of the GUID in the CHUID.	Noted. The GUID has always been a mandatory data element in the CHUID (see SP 800-73). In order to align with PIV-I, Revised Draft FIPS 201-2 requires that the GUID data element contain a UUID, just as is required for PIV-I.
SCA-16	Smart Card Alliance	Roger Roehr, Roehr Consulting	T	38	1188	4.1.4.4	Develop a Unique Person Identfier (UPID). In the FASC-N there are two parts: the first five fields (Agency,System,Credential,Credential Series, Individual Credential Issue) define the unique card ID and the last four fields identify the unique person identifier. When a credential is reissued a relying system can update an access account based on the last four fields of the FASC-N and not require a full re-enrollment. For PIV-I and universal use of the PIV, there is no Unique Person Identfier (UPID) in the data model. Access accounts do not have a unique ID that can be used for managing accounts.	4.2.4 Unique Person Identfier (UPID) This standard requires the inclusion of the Unique Person Identifier (UPID) as tag data element in the CHUID. The UPID will be an RFC4122 number that remains the same for a person the whole time the individual is affiliated with an issuer. This number will be used to update credential information in an access account when the credential has been reissued.	Resolved by AMAG-22.
SCA-17	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	E	43	1328	4.2.2	...The scope of the validation for the PIV Card shall include all cryptographic operations performed over both the contact and contactless interfaces. This is inconsistent with line 1372.	Change to:...The scope of the validation for the PIV Card shall include all cryptographic operations performed over both the contact and virtual contact interfaces.	Declined. Operations involving the symmetric and asymmetric Card Authentication keys may be performed over the contactless interface, even without secure messaging. In addition, cryptographic operations used to establish secure messaging (and the virtual contact interface requires the use of secure messaging) is also covered by this statement (i.e., cryptographic operations performed as part of secure messaging are within the scope of the validation, whether the secure messaging is performed over the contact or contactless interface).
SCA-18	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	T	3	283	1.3.4	When a feature is discontinued or no longer needed, it is deprecated. Such a feature remains in the current Standard as an optional feature but its use is strongly discouraged. A deprecated feature does not affect existing systems but should be phased out in future systems, because the feature will be removed inthe next revision of the Standard. For example, existing PIV Cards with deprecated data elements remain valid until they naturally expire. Replacement PIV Cards, however, should not re-use the deprecated features because the next revision of the Standard will remove the support for deprecated data elements.	Add: For backward compatibility, a deprecated data object shall remain in place and be populated with null values.	Declined. A deprecated feature or object will be still used as defined in the FIPS 201-1 to keep backward compatibility with the infrastructure compliant with FIPS 201-1.
SCA-19	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	G	8	476+	2.7	PIV-I cardholders applying for a PIV card should have a different process for identity proofing since they've already been through a proofing process for the PIV-I card.	Add: PIV-I, with an in-person validation, accepted as a sole proofing document in Section 2.7.	Resolved by CERT-10.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-20	Smart Card Alliance	Anna Fernezian, CSC	E	15	722	2.9.4	PIN reset at an unattended issuer-operated kiosk….biometric matches the stored biometric on the PIV card through either an on-card or off-card 1:1 biometric match… For PIN reset, it is assumed that the card is locked. This statement further assumes that OCC is available on the PIV card, since the 1:1 biometric match cannot be performed off-card as it is locked. Based on the written statements in lines 721 through 736, PIN Reset cannot be performed in unattended mode unless OCC is enabled. The 1:1 biometric match can be performed to reconnect the chain-of-trust (i.e., against the biometric stored in the IDMS).	Change lines 721-723 to read: PIN reset at an unattended issuer-operated kiosk shall ensure that the cardholder's biometric matches the stored biometric on the PIV Card, through either an on-card comparison or through performing a 1:1 biometric match of the cardholder with the biometric stored in the chain-of-trust record (i.e., IDMS/CMS), and that the PIV Card is authenticated.	Resolved by IL-4.
SCA-21	Smart Card Alliance	Anna Fernezian, CSC	E	15	736	2.9.4	Verification data *other than the PIN*…	Remove "other than the PIN"	Declined. The PIN is a form of verification data, but PIN reset is addressed in lines 709 through 735, so this sentence needs to note that the text beginning at line 736 only applies to verification data other than the PIN.
SCA-22	Smart Card Alliance	Anna Fernezian, CSC	T	42	1293	4.2.2	Asymmetric private key and corresponding public key to establish symmetric keys….	Could the Card Authentication Key be used to establish the symmetric keys, rather than create another certificate with additional policies?	Declined. This would be inconsistent with SP 800-57 Part 1, which states that a private key-establishment key shall not be used to perform signature operations. In addition, it would be insecure to use the Card Authentication key to establish symmetric key for secure messaging, as this would allow an attacker to obtain the symmetric keys be performing a replay attack. See also Cert-80 in the disposition of comments for the March 2011 Draft.
SCA-23	Smart Card Alliance	Tim Baldridge, NASA	T	8	460-475	2.6	Interagency transfer: a Federal employee is transferred from one agency to another. When the employee leaves the old agency, he/she surrenders the PIV Card and it is destroyed. When the employee arrives at the new agency and is processed in, the card issuer in the new agency requests the employee's chain-of-trust from the card issuer in the old agency, and receives the chain-of-trust. The employee performs a 1:1 biometric match against the chain-of-trust, and the interaction proceeds as described in Section 2.8.2.	Add: Cost savings and efficiencies may be achieved by accepting approved PIV-I issuers' enrollment data that is the PIV-I issuer chain-of-trust, excluding any the background investigation data which is intrinsically Governmental for PIV.	Resolved by FPKI-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-24	Smart Card Alliance	Tim Baldridge, NASA	T	8	455	2.6	The biometric data in the chain-of-trust shall be valid for at most 12 years. In order to mitigate ageing effects and thereby maintain operational readiness of a cardholder's PIV Card, agencies may require biometric enrollment more frequently than 12 years.	The biometric data in the chain-of-trust shall be valid for at most 12 years. In order to mitigate ageing effects and thereby maintain operational readiness of a cardholder's PIV Card, agencies may require biometric enrollment more frequently than 12 years. - Add: (Following line 455) Approved PIV-I issuer chain-of-trust data may be used by Federal Departments and Agencies for issuer identity proofing in meeting PIV registration requirements. A PIV-I issuer chain-of-trust shall include the enrollment and forensic data with respect to the PIV-I card issued to the new PIV applicant. A PIV-I issuer chain-of-trust shall not include background investigation data which is intrinsically Governmental for PIV. PIV-I issuers providing chain-of-trust data to PIV card issuers shall have available for inspection evidence of a qualified independent assessment of the PIV-I issuer adoption and use of and approved identity proofing and registration process in accordance with [SP 800-79]. Approved PIV-I issuer chain-of-trust data may be used by Federal Departments and Agencies for issuer identity proofing in meeting PIV registration requirements. A PIV-I issuer chain-of-trust shall include the enrollment and forensic data with respect to the PIV-I card issued to the new PIV applicant. A PIV-I issuer chain-of-trust shall not include background investigation data which is intrinsically Governmental for PIV. PIV-I issuers providing chain-of-trust data to PIV card issuers shall have available for inspection evidence of a qualified independent assessment of the PIV-I issuer adoption and use of and approved identity proofing and registration process in accordance with [SP 800-79].	Resolved by FPKI-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-25	Smart Card Alliance	Tim Baldridge, NASA	T	8	following line 475	2.6	Interagency transfer: a Federal employee is transferred from one agency to another. When the 470 employee leaves the old agency, he/she surrenders the PIV Card and it is destroyed. When the employee arrives at the new agency and is processed in, the card issuer in the new agency requests the employee's chain-of-trust from the card issuer in the old agency, and receives the chain-of-trust. The employee performs a 1:1 biometric match against the chain-of-trust, and the interaction proceeds as described in Section 2.8.2.	Interagency transfer: a Federal employee is transferred from one agency to another. When the employee leaves the old agency, he/she surrenders the PIV Card and it is destroyed. When the employee arrives at the new agency and is processed in, the card issuer in the new agency requests the employee's chain-of-trust from the card issuer in the old agency, and receives the chain-of-trust. The employee performs a 1:1 biometric match against the chain-of-trust, and the interaction proceeds as described in Section 2.8.2. Add: PIV-I for identity proofing: A Federal contractor working for a company where a PIV-I card is used as the company identification badge enters a new assignment that requires a PIV card. The contractor responds to an invitation for a PIV card application through a portal secured by the PIV-I card and authorizes the release of the PIV-I card issuer chain-of-trust data to the PIV card issuer. The PIV-I chain-of-trust data, including complete identification data, biometric images and templates, images as evidence of primary identity source document inspection, etc., is released to the PIV card issuer based on the applicant's approval. The PIV card issuer uses the biometrics and source documents from the PIV-I Issuer chain-of-trust. Upon completion of the background investigation in Section 2.7 and a cardholder 1:1 biometric match to connect to the PIV issuer's new chain-of-trust to the cardholder the PIV card issuer proceeds to issue a new card as described in Section 2.9.2	Resolved by FPKI-2.
SCA-26	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	G	42	1300	4.2.2	Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface.	Change to:..Any operation that may be performed over the contact interface of the PIV Credential may also be performed over the virtual contact interface.	Declined. This statement is making reference to the physical artifact (the card).
SCA-27	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	G	Throughout	Throughout	Throughout	Section 2.1 discusses Credential Control Objectives. However, the term PIV Card is frequently used throughout the revised draft. This removes the implied and unintended limitation of form factor and emerging technologies	Suggest replacing where appropriate the term PIV Card with PIV Credential or PIV Container or PIV Application. (see comment 35)	Declined. As specified in Sections 4.1 and 4.1.3, the limitation of form factor is neither implied nor unintended.
SCA-28	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	T	46	1441 -1444	4.2	Cardholder Identifiers Other identifiers may be present in credentials on the PIV Card that identify the cardholder rather than the card. Examples include the subject name and names that may appear in the subjectAltName extension in the PIV Authentication certificate. There needs to be a permanent PERSON identifier to specifically identify the cardholder that remains unchanged in the backend infrasturcture. This will simplify changes in the CREDENTIAL UUID or FASC-N that should occur at re-issuance as well as for BAE implementation.	Each PIV card contains a UUID and person Identifier PI that may be present in credentials on the PIV Card that identify the cardholder rather than the card. Examples include the subject name and names that may appear in the subjectAltName extension in the PIV Authentication certificate.	Resolved by AMAG-22.
SCA-29	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	E	60	1841 - 1848	6.3.1 Table 6-2	The sequence is non-intuitive to read; the highest level of assurance is at the bottom.	Reverse the stack sequence in the table	Resolved by XTEC-26.
SCA-30	Smart Card Alliance	Lars Suneborn, Hirsch-Identive	T	60	1599	6	Other authentication mechanisms than those described in Section 6 exist.	PIV authentication methods are not all inclusive and may at the discretion of the system owner use other authentication mechanisms.	Resolved by AMAG-24.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-31	Smart Card Alliance	Roger Roehr, Roehr Consulting	T	vii	195-196	10	A method that would allow post issuance updates to the PIV application will allow the total time for an interoperable capability to be deployed to be shortened. With the curent draft an agency can take up to year to develop a new requirement and six years before the requirement is fully implemented across the deployed base. With a post issuance update capabilty you could allow 24 months for development and certification and another 12 months for updating the deployed base and still be done in less than half the time of currently proposed timeline.	Change the sentence starting on line 195 to read, "To comply with FIPS 201-2, all PIV Cards shall comply with the mandatory PIV Card features no later than 36 months after the effective date of this Standard. It is highly recommended that PIV issuer develop a method to do post issuance updates to the PIV application."	Declined. There is no requirement for PIV Cards to be able to support post issuance updates, especially remote post issuance updates. In some case, it will be feasible for an issuer to add any newly mandatory data objects to a card when changing the contents of card for other reasons (e.g., rekeying certificates that are about to expire). Even if such a requirement were imposed, more time would need to be allowed. Furthermore, some of the PIV Card features that are made mandatory in FIPS 201-2 involve information that is printed on the card (e.g., the Zone 19F Card Expiration Date), and this cannot be addressed via a post issuance update.
SCA-32	Smart Card Alliance	Tony Damalas, Diebold	G	Glossary	1972	Appendix C		Add in the glossary a definition for PIV Credential and PIV Application	Resolved by replacing "PIV credential" with "PIV Card" in the first sentence of Section 4.2.4 and by replacing "credential identifiers" with "card identifiers" in the first bullet in Section 4.2.4. Declined to define "PIV Application" as this term does not appear in FIPS 201-2.
SCA-33	Smart Card Alliance	Tim Baldridge, NASA	G					Create definition for requirements for additional applications to coexist on a PIV card	Out of Scope. Card applications other than for the purpose of HSPD-12 / FIPS 201 is out of scope for this standard.
SCA-34	Smart Card Alliance	Tim Baldridge, NASA	T	46	1444	4.2.4	There is a need to expand the numeric identifier of the cardholder affiliation.	Each PIV card may contain an RFC 4122 generated 128-bit UUID that identifies the organization for the cardholder affiliation.	Resolved by AMAG-22.
SIA-1	SIA PIV WG	Rob Zivney	G	vii	190	9	Use of a feature is dependent on a sufficient number of cards in the population having the feature to use. In the case of optional features (on the card), there is therefore no interoperability for the readers and systems that use the card for that feature. Valuable new features introduced in FIPS 201-2 will likely not be usable on an interoperable basis for 15 years since a FIPS lifecycle (5 year minimum + draft and review) and a card population lifecycle (12 month exemption + 6 years) must both occur before the feature can be used. Nominal 15 year cycles for "use" are unacceptable as we hardly had the internet 15 years ago.	Revise the effective date of "optional" features to become "mandatory" to be upon the next issuance, reissuance, or renewal of cards or certificates, following publication of the relevant standards and publications.	Declined. If FIPS 201-2 were to state that "optional" features become mandatory upon the next issuance, reissuance, or renewal, then it would actually be making the feature mandatory and not optional. Features that are listed as optional to implement are optional, and there is not an implication that an optional feature will become mandatory in a later revision of the Standard (even though that is a possibility).
SIA-2	SIA PIV WG	Rob Zivney	G	vii	190	9	The FIPS 201-2 abstract states it is for an "architecture" for "technical interoperability" which indicates there is a systems level deliverable for "use," but the content of the document rarely goes beyond the card and the card edge. There needs to be guidance on the acceptable fallback operation of a reader/system using an optional feature or newly mandatory feature while cards without this feature are still in the general population of cards. Using the next lower assurance level, non-operation, or defaulting to the next higher level are all problematic and lead to non-usability. An "option" for the card is rarely an option for a reader/system that needs to know how to react when it encounters such an option in an environment expecting technical interoperability. An optional feature cannot be put to use, unless everyone implements the optional feature in all associated components.	Provide policy, guidance and reference to an appropriate standard or publication for the technical operation of a card with a reader/system when a desired option is not present in some components of the PIV ecosystem because it is or has been optional. Provide some statement to this effect in FIPS 201-2 so the GSA Evaluation Program can develop test procedures for certifying the acceptable non-interoperable behaviors associated with attempted use of optional features which are not present on the card.	Declined. Just as FIPS 201 does not mandate which authentication mechanism(s) a relying application must use, it does not specify how a relying application must address the situation in which the "primary" authentication chosen relies on data objects that may not be present on all PIV Cards and a cardholder with such a card needs access to the system. These are design decisions for the relying application.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-3	SIA PIV WG	Rob Zivney	T	v	119	3	HSPD-12 criteria is not met for defining "graduated criteria from least secure to most secure" since FIPS 201-2 only graduates up to 2 factor authentication when 3 factor assurance mechanisms are commercially available for Physical Access, and in fact used with the TWIC cards and readers.	Include 3 factor authentication as the most secure and show it as a graduated level above 2 factor authentication mechanisms throughout, but especially in Chapter 6 for Physical Access.	Declined. Section 6 describes a set of authentication mechanisms that may be implemented using the credential elements on PIV Cards. Three-factor authentication would require the implementation of more than one of these authentication mechanisms, and Section 6.3 already states that "the authentication mechanisms in Table 6-2 can be combined to achieve higher assurance levels," and references SP 800-116, which discusses the use of combinations of authentication mechanisms. See also CERT-18.
SIA-4	SIA PIV WG	Rob Zivney	E	vii	193	10	"Implementation" is a misleading word throughout this Standard. PIV Card features cannot be implemented until they are both mandatory in the card and mandatory in the associated reader/systems and the entire population of cards has been purged of PIV cards without this feature. Optional and Newly Mandatory features are not technically interoperable and therefore not usable unless they are present on all the cards and all the reader/systems for the agencies that choose to implement these features.	Change Title to Card Issuance and Component Functional Usage Schedule. Require that all cards be reissued within 4 years (12 month exemption + 3 year certificate life) and state that readers and systems must be prepared to use the Optional and Newly Mandatory features within 4 years.	Declined. The section is correctly labeled as it is specifying a schedule for implementing FIPS 201-2. Current PIV Cards may be valid for up to 5 years, so it would be unacceptable for FIPS 201-2 to require them to be replaced after 3 years. In addition, there is no requirement for readers and systems to be "prepared to use the Optional and Newly Mandatory features." A reader/system may, for example, be designed to authenticate cardholders using the PIV Authentication key and certificate, and there is no requirement that such a system be prepared to use any other card features (e.g., biometric data, CHUID data object, digital signature key, etc.).
SIA-5	SIA PIV WG	Rob Zivney	T	vii	203	10	This paragraph states that critical guidance "will be" outlined in FICAM. Similar wording as is used to establish effective dates for the New SPs needs to be used for FICAM, especially regarding newly mandatory and optional features prior to saturation availability in the PIV card population.	Add new paragraph for effective date of technically interoperable use of optional and newly mandatory features in the card.	Declined. The requirement is for PIV Cards that are issued after a certain date to include all of the mandatory features. There is no requirement for "technically interoperable use of optional and newly mandatory features in the card." (See SIA-4)
SIA-6	SIA PIV WG	Rob Zivney	T	22	922	3.2	There needs to be additional guidance that "usage" is only for "old" mandatory features and that usage depends on the available of the mandatory feature throughout the entire card population. Similarly a caution is necessary for all "optional" features. It is important to be clear that a card's usable lifecycle is dependent on the availability of mandatory features throughout the PIV ecosystem lifecycle.	Add asterisk to the PIV Card Usage block in Fig 3-2 with footnote: "Usage is a variable that can depend on the availability of mandatory, newly mandatory, and optional features throughout the entire card population. An individual card or agency usage may depend on how other agencies or sites or system components incorporate features."	Declined. Card features are usable even if they are not present on every PIV Card that is currently in use.
SIA-7	SIA PIV WG	Rob Zivney	T	42	1293	4.2.2	It is important that secure messaging be mandatory ASAP for the many beneficial features it enables, rather than wait two FIPS publication cycles (possibly 15 years).	State that "secure messaging" is a mandatory feature upon publication of the relevant SP.	Declined. Agencies may have a legitimate reason for choosing not to implement secure messaging (see DoD-1). If agencies agree that support for secure messaging provided "many beneficial features" then secure messaging will be widely implemented even if it is not mandatory.
SIA-8	SIA PIV WG	Rob Zivney	T	42	1298	4.2.2	The virtual contact interface is important to be mandatory ASAP rather than wait for two FIPS publications cycles (possibly 15 years). The requirements are not yet in SP 800-73 for the virtual contact interface.	State that the "virtual contact interface" is a mandatory feature upon publication or update of the relevant SP.	Resolved by SIA-7.
SIA-9	SIA PIV WG	Rob Zivney	E	46	1431	4.2.4	Suggest a short acronym be used for Authorization to distinguish from Authentication and Access be AuthN. Authorization should be AuthR, and Access as in ICAM remains A. I&A herein is inconsistent.	Change I&A to I&AuthN.	Declined. I&A is used consistently in FIPS 201-2 to mean "Identification and Authentication." This is not inconsistent with the FICAM Roadmap, with uses "IA" to stand for "Identification and Authentication."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-10	SIA PIV WG	Rob Zivney	T	46	1433	4.2.4	If Authorization occurs, Authentication is actually a step in the Authorization process. For "performance," Authorization process engines might not even execute Authentication as the first step. Current wording can indicate prescription for how the Authorization processes are executed and that is undesirable, especially if it gets caught in the traceability matrix of the GSA Evaluation Program.	Add a footnote: Authentication is a step in the Authorization process and need not be the first or prerequisite step in executing the Authorization process.	Declined. Authentication is not necessarily a step in the authorization process, as the authorization process may be designed to accept an authenticated identity as input. The text in Section 4.2.4 does not indicate that authentication must be performed as a first step, nor does it preclude skipping the authentication process altogether in cases in which the presented identity is not authorized. It merely notes that a decision to grant authorization that is based on a presented identifier cannot be made before the identity has been authenticated.
SIA-11	SIA PIV WG	Rob Zivney	T	46	1438	4.2.4	The UUID is not an apples-to-apples equivalent of the FASC-N. The FASC-N does contain a Credential Identifier, but it also contains a Person Identifier which has relevance via the Organization Identifier. A mechanism needs to be present to provide 3 different UUID. Many Back End Attributes are associated with the person in an organization and has a lifecycle of the person whereas the card and certificate have shorter lifecycles. PACS that perform Role Based Access Control manage many access privileges based on the person identifier; however enterprise applications would otherwise need a broker to manage the ongoing association between the person and their many possible credentials and certificates.	Establish 3 UUID to be equivalent to the FASC-N, and include a Credential UUID, a Person UUID, and an Organization UUID.	Resolved by AMAG-22. Additional identifiers may be considered during SP 800-73 revision
SIA-12	SIA PIV WG	Rob Zivney	T	52	1594	6	Unless the permissible is specifically acknowledged, the procurement officer and the GSA Evaluation Program's traceability matrix process will assume "not permitted." More explicit acknowledgement of permissible mechanisms are necessary, even if accompanied by an associated statement of a valid authentication factor being out of scope.	Add a footnote: PIN to PACS is an acknowledged valid authentication mechanism if applied in accordance with EPACS as published by the CIO Council, and required by DCIDS 6/9, now ICD 705.	Resolved by AMAG-24.
SIA-13	SIA PIV WG	Rob Zivney	T	52	1615	6.1	OMB-04-04 was published prior to HSPD-12 and though a starting point, is not sufficient to meet the HSPD-12 requirement for "graduated criteria from least secure to most secure." OMB-04-04 and SP 800-63 are only for logical access and only for remote authentication. Further these only deal with the science of cryptography which excludes biometrics since they are not secrets. SP 800-63 is inherently limited to 2 factor assurance when 3 factor assurance is commonly used in government and non-government physical access application for the more/most secure applications. OMB-04-04 may be the "basis," but HSPD-12 is the mandate. This section reads as if NIST is limiting physical security solutions to align with logical security implementation challenges rather than address National Security needs.	Bring FIPS 201-2 into compliance with HSPD-12 for physical access by including 3 factor assurance mechanisms. Use the state-of-the-art, field proven TWIC model as a basis for physical security in high security and outdoor environments. Reference E-PACS from the CIO Council for additional guidance. Acknowledge in FIPS 201-2 that OMB M-04-04 is not for physical access, but rather ONLY remote logical access. Add reference to footnote 7, page 20 of SP 800-63-1.	Resolved by Cert-18.
SIA-14	SIA PIV WG	Rob Zivney	T	52	1620	6.1	This line is technically inaccurate in light of the HSPD-12 requirements for most secure. It might provide strong assurance of the legitimacy of the card but without establishing a stronger binding between the credential and the cardholder simple PIN triggered PKI is not that secure. It is too easy to shoulder surf a PIN and steal a card. This standard establishes biometrics as essential to enroll and be issued a card but ignores biometrics as essential for the highest assurance level in use of the card without the prohibitively expensive guard standing at every reader.	Make HSPD-12 the basis for FIPS 201-2 rather than OMB-04-04 and SP 800-63.	Noted. HSPD-12 is the basis for FIPS 201-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-15	SIA PIV WG	Rob Zivney	E	53	1648	6.2.1	There is an acronym for On Card Comparison, but not one for Off Card Comparison. Use of OCC is too confusing as to which it is.	Revert to BMOC for Biometric Match On Card or use OnCC and OffCC.	Declined. See IBIA-1b in the disposition of comments for March 2011 Draft FIPS 201-2. As OCC is used consistently in FIPS 201-2 to mean on-card biometric comparison, there is no reason to believe that reader would be confused about the meaning of this acronym.
SIA-16	SIA PIV WG	Rob Zivney	T	54	1663	6.2.11	There are too many choices (effect options) for the GSA Evaluation Program to test when it comes to selecting various data elements for comparison and input to the Authorization engine.	Be more specific as to which data elements are checked for what. Write language as if YOU were doing the testing for interoperability and conformance.	Declined. In many cases a pre-existing system will be PIV enabled, and the requirements of the system will dictate what data needs to be provided to make the authorization decision (e.g., a system based on Active Directory will make authorization decisions based on a User Principle Name, regardless of what FIPS 201-2 might say). See also comment AI-23, Cert-106, SCA-68, SCA- 103 in the disposition of comments from the March 2011 Draft FIPS 201-2.
SIA-17	SIA PIV WG	Rob Zivney	T	59	1822	6.3	If it is permissible to combine PKI-AUTH and BIO for a "higher" degree of assurance in cardholder identity, show it in table 6-2 and give it a name else, the implementer will think that the Most Secure level can be met with only 2 factor authentication. Further, without this 3-factor combination in the table, the GSA Evaluation Program might not create a category for this essential reader combination and the consumer might not find it tested for conformance, etc.	Add another row to the end of Table 6-2 called HIGHEST Assurance and list BIO + PKI-AUTH	Resolved by SIA-3.
SIA-18	SIA PIV WG	Lars S	T	60	1841- 1848	6.3.1 Table 6-2	There are four levels of assurance with one, two or three authentication mechanism alternatives for each level. However there is no mention of when a combination of one, or two authentication mechanisms may be used. Suggest adding in the High Confidence row (PKI-CAK + PIN-to-PACS) and (SYM-CAK + PIN-to-PACS) This will provide additional flexibility as well as control functions such as elevator control, IDS and Video control to name a few examples	In the High Confidence row , add: (PKI-CAK + PIN-to-PACS) and (SYM-CAK + PIN-to-PACS)	Resolved by AMAG-24 and SIA-3.
SIA-19	SIA PIV WG	Lars S	E	60	1841- 1848	6.3.1 Table 6-2	The sequence is non-intuitive to read; the highest level of assurance is at the bottom.	Reverse the stacking sequence so thet the highest level of assurance is on top	Resolved by XTEC-26.
SIA-20	SIA PIV WG	Lars S	T	2	272	1.3.3	New features are optional or mandatory features that are added to the Standard. New features have been field proven to interfere with backward compatibility because they are not part of the existing systems.	Add Caution: New features may interfere with backward compatibility because they are not part of or anticipated in the existing systems.	Declined. Existing relying systems will simply ignore the presence of new features and so will not be impacted.
SIA-21	SIA PIV WG	Rob Zivney	G				It is not clear when an optional feature of the card becomes a mandatory feature for the readers and system that use the card.	Provide an effective date for readers and systems to begin using an optional feature of the card.	Resolved by SIA-4.
SIA-22	SIA PIV WG	Rob Zivney	G				It is not clear when a newly mandatory feature of the card becomes a mandatory feature for the readers and system that use the card.	Provide an effective date for readers and systems to begin using a newly mandatory feature of the card.	Resolved by SIA-4.
SIA-23	SIA PIV WG	Rob Zivney	T	21	880	3.1.1	In addition to "something you have," "something you know," "and something you are," there is a fourth factor: "something someone else knows about you." Like an electronics notary public, checking a certificate's validity provides a functional distinguishable factor from something you have.	Include the 4th authentication factor "something someone else knows about you."	Declined. As noted in SP 800-63-1, there are three recognized authentication factors: "The three types of authentication factors are something you know, something you have, and something you are." "Something someone else knows about you" is not a recognized authentication factor.
SIA-24	SIA PIV WG	Adam Shane	G	3	282	1.3.4	While it is understood that re-use of deprecated features seems like good change management, this is a significant challenge for relying party systems. Deprecated features are not backward compatible, and this section even indicates that such features remain in the standard.	If deprecated features remain optional in the standard, there is no reason to remove them on replacement of the card. Remove statement from standard.	Resolved by AMAG-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-25	SIA PIV WG	Adam Shane	T	3	287	1.3.5	Other components that may be affected by version management include components or systems that rely on PIV cards or their data.	Add to the last sentence of the paragraph, "and components or systems that rely on PIV cards or their data."	Resolved by AMAG-3.
SIA-26	SIA PIV WG	Adam Shane	T	7	429	2.5	The standard allows for use of electronic facial image for authentication in operator-attended PIV issuance, but does not consider use of this authentication mechanism for use in PACS.	Statement at line 429 should be expanded to add, "or other operator-attended authentication operations."	Resolved by AMAG-6.
SIA-27	SIA PIV WG	Adam Shane	E	12	606	2.9	"PIV card update" is referred to as PIV card renewal in following section 2.9.1.	Section 2.9 should be updated for consistency.	Resolved by AMAG-7.
SIA-28	SIA PIV WG	Adam Shane	T	13	628	2.9.1	If the original PIV card is lost, stolen between time renewal is requested and time card is issued, then the card cannot be surrendered. However, it would be inefficient and expensive to abandon the renewal process and start a re-issuance process at that time (HSPD-12 refers to government efficiency).	In line 628 "shall" is to be replaced by "should", and the statement to be augmented with direction to revoke certificates and other appropriate operations if the card is not available for surrender.	Resolved by AMAG-11.
SIA-29	SIA PIV WG	Adam Shane	T	13	635	2.9.1	The standard states that biometric authentication accuracy degrades with time elapsed since initial collection. I don't believe this is a generally held belief. If NIST has empirical studies to back up this statement they should be referenced in a footnote.	Remove the offending statement. It becomes a policy decision, not based on scientific data but on a desire to limit risk.	Resolved by AMAG-9.
SIA-30	SIA PIV WG	Adam Shane	T	13	639	2.9.1	If the PIV Authentication Key is designated as a person authentication, then it should not be re-issued when a new PIV card is created. The CAK on the other hand is a card authentication key and should be re-issued. Furthermore, if certificates are re-issued, then the older certificates should be revoked.	Section 2.9.1 should be updated to include the revocation of the old keys if new keys are issued.	Resolved by AMAG-10.
SIA-31	SIA PIV WG	Adam Shane	T	14	689	2.9.3	Part of Agency policy should be to notify the individual when data on their PIV card changes. They should be notified of what changed, and why.	The standard should be updated to require Agencies to modify their privacy policy to notify individuals when their PIV card data is modified, and when backend systems data about them is modified.	Resolved by AMAG-12.
SIA-32	SIA PIV WG	Adam Shane	G	15	708	2.9.4	IT best practices indicate PIN reset should be done every 90 days. In case of existing PIN being known, OCC not required - 2.9.4 assumes PIN is forgotten, but perhaps generically Card Data Reset should require three-factor authentication.	NIST to consider how to bring PIV card into compliance with 90-day PIN reset recommendations. 2.9.4 should require three-factor authentication.	Resolved by AMAG-13.
SIA-33	SIA PIV WG	Adam Shane	T	16	749	2.9.5	A negative background investigation report received after the issuance of the card should be cause for card termination. Also, if agency uses Continuous Information Management Engine (CIME) and it returns negative information, this may also be cause for card termination.	Update 2.9.5 to include additional reasons that may be cause for PIV Card Termination.	Resolved by AMAG-14.
SIA-34	SIA PIV WG	Adam Shane	E	16	759	2.9.5	It is not clear what it means to "revoke" a PIV card. Does this mean the certificates are revoked? Or should this term be changed to "terminated" as it is used on lines 775 and 776?	This statement should be modified or clarified.	Resolved by AMAG-15.
SIA-35	SIA PIV WG	Adam Shane	E	17	788	2.11	HSPD-12 does not say that the control objectives are the only applicable uses of the PIV card.	NIST should not be changing the meaning of HSPD-12. The statement should be removed or modified to state, "No department or agency shall implement a use of the identity credential that is in contradiction to any of these control objectives."	Resolved by AMAG-16.
SIA-36	SIA PIV WG	Adam Shane	T	18	818	2.11	Employees should not be making the decision to protect their PIV data through an electromagnetically opaque holder. This should be a CPO decision that flows into Agency policy.	Modify the statement to read, "Specifically, Agencies may choose to deploy PIV credentials with electromagnetically opaque holders…"	Resolved by AMAG-17.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-37	SIA PIV WG	Adam Shane	E	20	861	3.1.1	Card readers are also located at registration and issuance stations.	Update the statement.	Resolved by AMAG-18.
SIA-38	SIA PIV WG	Adam Shane	T	55	1706	6.2.3.1	This section states that the reader validates the certificate. In the case of a transparent reader, it is not the reader but some other component of the system that is performing the validation. This is also found in 6.2.3.2 at 1726.	This section is normative so it will be interpreted that it must be implemented in this fashion. The statement should be updated to indicate that the system performs the validation, and not any specific component.	Resolved by AMAG-32.
SSA-1	SSA	Matthew D. Meyer	G	vii	194-199	Preface 10.	**The 12-month compliance period is too short.** Agencies will require longer than 12 months for compliance with FIPS-201-2 when finalized. Three years would be more realistic. It has been said that agencies can start implementing the additional requirements now instead of waiting for the finalization of this FIPS. However, there is much work to be done in terms of publishing and updating special publications, vendor product updates and re-certifications, agency acquisition and deployment, etc. The direction that FIPS-201-2 sets is a solid direction, but agencies will realistically require additional time to comply with the standard. Note the following: o This FIPS is just not saying that previously optional elements are now mandatory, the content of these elements is also changing. For example, the UUID/GUID will now be required in certain certificates and in the biometrics. o Additional certificates require additional issuance time, very noticeable to the end user if you have not been doing this from the beginning. o On-Card facial image format requires additional resolution/quality and that requires re-training of enrollers, greater attention to environmental factors, in addition to software changes.	Make the compliance period three years rather than one year.	Resolved by DoD-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SSA-2	SSA	Matthew D. Meyer	T	74	2301-2304	Appendix D	**This FIPS references special publications that are not yet published or which need to be updated.** The second public draft of FIPS-201-2 references two special publications, SP800-156 and SP800-157, which are not yet published, even in draft form. Moreover, this FIPS will require updates to special publications such as 800-73 that are not yet available. However, agencies are required to submit comments this week (8/10) and this is the last time comments on this FIPS will be accepted. We find it difficult to fully analyze and comment on this FIPS when such references are unavailable. Of specific concern is the lack guidance on derived credentials when combined with the new requirement to issue the Key Management Certificate to all with a .gov email account. This leaves critical gaps in the approved approach to data and key recovery when typical email usage scenarios with a combination of a PC and Blackberry are considered.	With understanding that it is easier to publish an SP as opposed to a FIPS, the following actions are recommended : o Extend the time for which agencies are required to comply with FIPS-201-2 to three years from the finalization date. This allows time for the SPs to be published, commented-on, and finalized. Keep in mind vendors will need to update their product offerings based on the SPs, and agencies will need time to acquire, integrate, and deploy these updates. Consider starting the compliance clock based on the finalization or update of all the SPs referenced in this FIPS. o Relax the requirement for agencies to issue the Key Management Certificate to everyone with an email address. In this way you stay out of hot water with execs not being able to read encrypted email on their Blackberry and coming down hard on the HSPD-12 office as a result.	o Resolved by SSA-1. There would be no reason to start the compliance clock based on the finalization or update of all the SPs referenced in FIPS 201-2 since everything that is mandatory-to-implement in FIPS 201-2 is already fully specified in either FIPS 201-2 or the current versions of the referenced SPs. While it will not be possible to implement the new features of FIPS 201-2 until the related SPs have been published or updated, these features are optional-to-implement, and so the 12-month time frame is not relevant for them. o Declined. SP 800-157 is not required to address the issue of using the key management key to decrypt messages on devices that do not have card readers, as this is not related to the issuance of derived credentials. The ability to decrypt emails requires that the same credential be available in all places, not a derived credential. There is nothing in FIPS 201-2 or [COMMON] that precludes the key management private key from being stored on more than one device (e.g., the PIV Card and a Blackberry) as long as the requirements of [COMMON] are satisfied. In many cases, this will involve issuing the key management certificate under id-fpki-common-policy rather than id-fpki-common-hardware or id-fpki-common-High, as id-fpki-common-policy is the only policy that would permit the private key to be stored in a FIPS 140 Level 1 software cryptographic module.
SSA-3	SSA	Matthew D. Meyer	T	41	1248	4.2	**The Key Management Certificate should continue to be an optional data element.** Agencies should not be required to issue the Key Management Certificate to all with a .gov email address. This opens up a huge can of worms in terms of data and key recovery, and the current key recovery capabilities in the PIV space are simply not good enough for mass use in all environments. Even the latest PIV cards can only hold 5 historic key management certificates before you start getting into off-card storage, which is not well supported. Use of PKCS12 file recovery mechanisms puts tension on “hardware” policies, and requires more technical sophistication on behalf of the user. Agencies that do issue Key Management Certificates to all users have noted the time and expense spent on key recovery cases. Agencies may wish to use other mechanisms to provide for confidentiality for data on the wire and at rest, mechanisms that do not rely on the traditional notions of per-user key recovery and escrow. Many are now employing more efficient key management system for data at rest, and those principles can be extended to electronic mail in time, including mail on mobile devices, saving us all the headaches of traditional asymmetric private key recovery.	Keep the Key Management Certificate optional.	Declined. As noted in the Federal Register notice for Revised Draft FIPS 201-2, the key management key was made mandatory for cardholders who have government-issued email accounts at the request of OMB in order to align the Revised Draft FIPS 201-2 with the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance. OMB Memorandum M-11-11 also states that 'The government-wide architecture and completion of agency transition plans must align as described in the Federal CIO Council's “Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance” (available at www.idmanagement.gov).' See also SSA-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SSA-4	SSA	Matthew D. Meyer	T	2	248-249	1.2	**Guidance on temporary and visitor credentials should be provided in this FIPS or a companion special publication.** It is unfortunate that guidance on temporary PIV credentials is still not provided in this FIPS. For largely distributed agencies, like SSA with 1600 issuing locations, on-site card printing is simply not feasible given the state and expense of current smart card printing technologies. So, we and other agencies, and the MSO, use the Oberthur Bureau Printing, or some form of central printing. This does add some delays for replacement card shipping. We've developed and are deploying a temporary card process to take care of these gaps, allowing a user, for instance, to continue to utilize smart card logon or a PIV-enabled VPN solution in the interim. SP800-116 indicates that we can kind of do what we want for credentials with lifetimes under 6 months. But what does that really mean? Does it mean I can use Common Policy / PIV OIDs in the short term certificates? If I don't then the card may not be functional for certain applications, especially those outside of the agency, that may require those OIDs. Should I have to run a completely separate PKI for these type of cards and certificates? If so, why am I paying for an SSP as well? Perhaps this could be covered in the coming guidance on "derived credentials" since we are issuing the temp to the user's same PIV identity. Consider also some corresponding additional guidance for visitor credentials. There is clear direction now to use the Card Authentication Certificate as the basic contactless authentication mechanism for PACS. But no increase in security is gained if someone can forge a prox card and use that at another turnstile, posing as a visitor, or posing to have some temporary card. So, if we are really going to do this, then every form of card, PIV permanent, PIV temporary, visitor temporary, should really have some form of card authentication or card-auth-like certificate, and that should be stated somewhere in this FIPS or a companion special publication (157, 116), so there is no wiggle-room on what really makes a secure solution. Vendors can then implement solutions based on such guidance that agencies can acquire and deploy.	Provide clearer guidance on temporary credentials in this FIPS or a companion SP.	Declined. FIPS 201 is the Standard for issuing "secure and reliable forms of identification" for federal employees and contractors under HSPD-12 and as further clarified in OMB M-05-24. Temporary and visitor credentials fall outside of that scope. Common Policy OIDs may only be asserted in certificates that are issued in accordance with the requirements specified in [COMMON]. PIV OIDs (those specified in FIPS 201) may not be used other than on PIV Cards, except in cases in which explicit permission has been granted (as was done with the id-PIV-cardAuth extended key usage OID and PIV-I cards). It is understood that systems that have chosen to only accept PIV Cards will not accept cards that are not PIV Cards (e.g., temporary and visitor credentials).
SSA-5	SSA	Matthew D. Meyer	T	15	725-731	2.9.4	**The requirement for a biometric match on-card for a remote PIN reset is not realistic.** The card stock that even has the biometric match on card functionality is not well –distributed, and there are plenty of cards out there under the older standards and they are still good for another couple of years. It's not feasible to field compliant biometric scanners to every remote worker. Many remote workers, who work at home all the time, are disabled, will have trouble with the fingerprint functionality. So you're essentially forcing agencies to adopt a non-compliant remote reset procedure for operational continuity reasons and to accept that risk. Any level of compliance with this would certainly go well beyond the 12-month requirement.		The remote PIN reset is a new capability that was added based on significant demand. This text is not imposing a new requirement for which agencies are expected to become compliant within the 12 months of the effective date of FIPS 201-2, it is a new option. FIPS 201-1 says: "PIN resets may be performed by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card." Resetting the PINs on PIV Cards without performing a biometric match of the cardholder is not in accordance with FIPS 201-1. PIV Cards must satisfy the requirement in HSPD-12 that they be "secure and reliable forms of identification." Thus, any procedure to reset the PIN on a PIV Card must provide a sufficient level of security. See also DoD-18.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
TR-1	Treasury	Jim Walker	T	42	1290-1292	4.2.2	Does making the digitial signature and key management keys mandatory on the PIV card also speak with policy Object Identifiers (OIDs) for these certificates? For example, if they are mandatory on the card - do they also have to assert a hardware only OID?	Add a statement asserting the expected Certificate Policy Object Identifier (OIDs) for these keys.	Noted. This information already appears in Section 5.2.1, with additional information for legacy PKIs being provided in Section 5.4.
TR-2	Treasury	Jim Walker	G	16	773-776	2.1	A solid timeline is needed for derived credentials. It was explained during the workshop that FIPS201-2 and two other, un-named, higher priority special publications would be completed prior to 800-157 being started. Given that mobile devices are increasingly being pushed/used in the federal workplace - guidance for how to PIV enable them is critical and a barrier to fully requiring PIV in the enterprise.	Provide guidance on PIV enabling on mobile devices (to include timeline).	Noted. It was stated at the workshop that development of SP 800-157 was considered to be very high priority, and that work on it would precede work on other, lower priority documents. While a timeline for the development of SP 800-157 cannot be provided, the development is SP 800-157 is not considered to have lower priority to the development of any other document.
TR-3	Treasury	Ivelisse Galarza-Pagan	G	Not availabl e	Not available	Not available	– The separate section on re-key has been deleted. **Comment:** How post issuance actions/activities be differenciated from Rekeys, Card Updates and Reprints?	Provide clarification on post issuance actions/activities.	Declined. As noted in Section 2.9.3 (now Section 2.9.2), changing the keys on a PIV Card (rekey) is a form of post issuance update, so there is no need to differentiate rekeys from post issuance updates. The term "reprint" does not appear in FIPS 201, however, the term "reprint" seems to imply the creation of a new PIV Card, which is not the same as a post issuance update, since a post issuance update involves changing the data that is stored electronically on the card, not issuing a new card.
TR-4	Treasury	James Moloney	G	vii	175-176	8	The contactless free read option is not currently available and is the only viable LACS accommodation for employees without full use of their hands. When will this be available and what is the recommended workaround?	Provide guidance for logical access accomodations for employees without full use of their hands.	Declined. As noted in FIPS 201-2, the Standard describes authentication mechanisms that are supported by PIV Cards, however, it is the responsibility of individual departments and agencies to choose the appropriate authentication mechanisms for their systems, including ensuring that appropriate accommodations are provided for those with disabilities.
TR-5	Treasury	James Moloney	G	vii	190-192	9	Optional features are said to be backward compatable and standards are detailed in special publications. The Special Publications are not completed in most cases and in some the publication is not even started. How can these optional items be backward compatible without a standard to follow? Venders will not expend resources to develop these optional features without some guidance. There is not even any assurance that the feature will be an optional feature in the next version of FIPS 201	Optional features should not be indentified without supporting Special Publications.	Noted. The introduction of a new, optional item is considered backward compatible since existing relying system will be able to work with new cards that implement the item (the existing systems will simply ignore the existence of the new item on the cards). We would strongly discourage vendors from expending resources to develop features before the technical details for those features have been fully specified in the relevant Special Publication(s). As noted in the Effective Date section, "New optional features of this Standard that depend upon the release of new or revised NIST Special Publications are effective upon final publication of the supporting Special Publications." Each revision to FIPS 201 will be made with substantial consideration given to input provided by agencies and other interested parties. A feature that is optional-to-implement in FIPS 201-2 may be made mandatory-to-implement in FIPS 201-3 if NIST receives significant input arguing that the feature should be made mandatory-to-implement. However, it would be impossible for NIST to predict at this time what comments might be submitted during the next review cycle for FIPS 201.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
TSCP-1	TSCP		G	viii	194-197	10	It is not clear whether this is a requirement for switch-over of issuing or for all cards to comply within 12 months		The referenced text states: "This Standard mandates the implementation of some of the PIV Card features that were optional to implement in FIPS 201-1. To comply with FIPS 201-2, all new and replacement PIV Cards shall be issued with the mandatory PIV Card features no later than 12 months after the effective date of this Standard." PIV Cards that are issued before the effective date of FIPS 201-2, or that are issued within the first 12 months after the effective date of FIPS 201-2, may continue to be used until they expire or need to be replaced for some other reason (e.g., the become lost, stolen, damaged, or compromised, or some data on the card needs to be changed and the change cannot be made via a post issuance update).
TSCP-2	TSCP		G	29	1084-1089	4.1.4.1	How is this zone used in the case of a foreign national contractor?		Line 1090 states "Foreign National color-coding has precedence over Government Employee and Contractor color-coding." Thus, in the case of a foreign national contractor, the Zone 15F color-coding would be Blue to indicate foreign national.
TSCP-3	TSCP		E	75	2309	Appendix D	Broken link prevents review of link to secure e-mail		Noted. We have informed the web administrator for Idmanagement.gov, and have also updated the URL based on the reorganization of the idmangement.gov web site.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
TSCP-4	TSCP		G	7	460-475	2.6	Cost savings and efficiencies may be achieved by accepting approved PIV-I issuers enrollment data that is the PIV-I issuer chain-of-trust, excluding any the background investigation data which is intrinsically Governmental for PIV.	(Following line 455) Approved PIV-I issuer chain-of-trust data may be used by Federal Departments and Agencies for issuer identity proofing in meeting PIV registration requirements. A PIV-I issuer chain-of-trust shall include the enrollment and forensic data with respect to the PIV-I card issued to the new PIV applicant. A PIV-I issuer chain-of-trust shall not include background investigation data which is intrinsically Governmental for PIV. PIV-I issuers providing chain-of-trust data to PIV card issuers shall have available for inspection evidence of a qualified independent assessment of the PIV-I issuer adoption and use of an approved identity proofing and registration process in accordance with [SP 800-79]. (Following line 475) PIV-I for identity proofing: A Federal contractor working for a company where a PIV-I card is used as the company identification badge enters a new assignment that requires a PIV card. The contractor responds to an invitation for a PIV card application through a portal secured by the PIV-I card and authorizes the release of the PIV-I card issuer chain-of-trust data to the PIV card issuer. The PIV-I chain-of-trust data, including complete identification data, biometric images and templates, images as evidence of primary identity source document inspection, etc., is released to the PIV card issuer based on the applicant's approval. The PIV card issuer uses the biometrics and source documents from the PIV-I Issuer chain-of-trust. Upon completion of the background investigation in Section 2.7 and a cardholder 1:1 biometric match to connect to the PIV issuer's new chain-of-trust to the cardholder the PIV card issuer proceeds to issue a new card as described in Section 2.9.2	Resolved by FPKI-2.
XTEC-1	XTec Incorporated	Rick Uhrig	G	All	All	All	The term "credential" seems to be used with multiple meanings in the document, leading to ambiguity and, for some readers, confusion. Within the standard "credential" occurs 145 times in at least 17 different forms (credential, PIV Credential, identity credential, logical credential, credential identifier, derived credential, credential number, electronic credential, visual credential, certificate credential, stored credential, PKI credential, issued credential, general credential, special-risk credential, security credential, credential element). Sometimes it seems like the "credential" is referring to the PIV Card in its entirety (e.g. 2.1 Control Objectives, Springer Memo, OMB reporting requirements) and sometimes to visual or logical elements on the PIV Card such as a certificate, CHUID or PIN. This vague use and the many different forms it appears in create a ambiguity and uncertainty, which in turn leads to different interpretations as to what the standard requires.	Tighten-up the use of the term "credential." Explicitly state that the PIV Card is the credential for the purposes of the Springer memo and OMB reporting. (Don't want to report all PIN resets to OMB after all.) Otherwise, prefer "PIV Card" rather than "credential" or "PIV credential" where that is meant. Specifically list the logical credentials. Either get rid of the term "credential element" or explain why this notion is necessary. Replace "PIV Credential" by "PIV Card", "logical credential" or just "credential", whichever is meant. Extra Credit: Gather the surviving set of "credential" terms together and compare and contrast, so the subtleties of what is intended by each become clear. (The more challenging this is for NIST experts, the more essential it is for the average reader)	Resolved by replacing some instances of "credential" with "PIV Card," where appropriate.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
XTEC-2			T	2	250	1.3.1	The definition for backward compatible changes is one-side. It categorizes compatibility only in terms of existing systems, but not in terms of existing PIV Cards.	Change to: "A backward compatible change is a change or modification to an existing feature that does not break the systems **or PIV Cards** using this feature. For example, changing the Card Authentication certificate from optional to mandatory does not affect the systems using the Card Authentication certificate for authentication (i.e., using the PKI-CAK mechanism)."	Decline to remove one-sided nature of description of a backward compatible change. Guidance needs to be provided to implementers of relying systems on the potential impacts that changes to the specification of the PIV Card in the Standard may have on their systems. The effects that changes to aspects of the Standard that relate to relying systems may have on the ability of relying systems to continue to interoperate with existing PIV Cards is an issue that is addressed as part of the standards-development process. Intent clarified by changing the first sentence of the second paragraph of Section 1.3 to: This section provides change management principles and guidance to implementers of relying systems to manage newly introduced changes and modifications to the previous version of this Standard. and by changing the first sentence of Section 1.3.1 to: A backward compatible change is a change or modification to an existing feature that does not break the relying systems using this feature.
XTEC-3	XTec Incorporated	Rick Uhrig	T	2	264	1.3.2	The definition for non-backward compatible change is one-side. It categorizes non-backward compatibility only in terms of existing systems, but not in terms of existing PIV Cards.	Change to: "A non-backward compatible change is a change or modification to an existing feature such that the modified feature cannot be used with existing systems **or existing PIV Cards**. For example, changing the format of the biometric data would not be compatible with the existing system, because a biometric authentication attempt with the modified format would fail. Similarly, changing the PIV Card Application Identifier (AID) would introduce a non-backward compatible change. As a result, all systems interacting with the PIV Card would need to be changed to accept the new PIV AID. Also, the requirements specified in Section 2.9.4 for Remote PIN Reset are non-backward compatible, since this feature does not work PIV Cards that do not support OCC (all existing PIV Cards). Thus, any change to an existing Remote PIN Reset Capability to enforce the requirements of 2.9.4 will necessarily not work with existing PIV Cards and is non-backward compatible. "	Resolved by XTEC-2. Intent of Section 1.3.2 clarified by changing the first sentence of the section to: A non-backward compatible change is a change or modification to an existing feature such that the modified feature cannot be used with existing relying systems. Note: The requirements specified in Section 2.9.4 (now Section 2.9.3) for remote PIN reset cannot be categorized as a non-backward compatible change since remote PIN reset is not supported by FIPS 201-1 (i.e., there cannot be an existing remote reset capability that conforms to the requirements specified in FIPS 201-1 for PIN reset).

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
XTEC-4			T	2	277	1.3.3	New features for PIV Cards do not interfere with backward compatibility. However, new features for systems will interfere with backward compatibility if these features negate existing functionality that works with existing PIV Cards.	Change to: "New features are optional or mandatory features that are added to the Standard. New PIV Card features do not interfere with backward compatibility because they are not part of the existing systems. For example, the addition of an optional on-card biometric comparison (OCC) authentication mechanism is a new feature that does not affect the features in current systems. The systems will need to be updated if an agency decides to support the OCC-AUTH authentication mechanism. However, new relying system features may interfere with backward compatibility. For instance, the new feature for Remote PIN Reset that requires PIV Card OCC is not backward compatible. Any existing implementations of Remote PIN Reset, once upgraded to require OCC, will no longer work with existing PIV Cards."	Resolved by XTEC-3. Intent of Section 1.3.3 clarified by changing the second sentence of the section to: New features do not interfere with backward compatibility because they are not part of the existing relying systems.
XTEC-5			T	3	282-283		The statement "Replacement PIV Cards, however, should not re-use the deprecated features because the next revision of the Standard will remove the support for deprecated data elements" reflects the current one-sided bias of backward and non-backward compatibility in the draft. In the real world, to assure smooth change management, exactly the opposite advice should be given.	Change to "Replacement PIV Cards must also continue to re-use the deprecated features as long as the issuer's or other relying parties' systems continue to require those features. All parties must begin to migrate their relying systems to NOT use the deprecated features because the next revision of the Standard will remove the support for deprecated data elements"	Resolved by replacing Section 1.3.4 with: When a feature is to be discontinued or is no longer needed, it is deprecated. In general, a feature that is currently in use by relying systems would only be deprecated if there were a compelling (e.g., security) reason to do so. Deprecated features may continue to be used, but should be phased out in future systems since the feature will likely be removed in the next revision of the Standard. For example, the CHUID authentication mechanism (Section 6.2.5) has been deprecated, since it provides LITTLE or NO assurance in the identity of the cardholder, and so relying systems should phase out use of this authentication mechanism. In the case of deprecated features on PIV Cards, such as the authentication key map, existing PIV Cards with the deprecated features remain valid, however, new PIV Cards should not include the deprecated features.
XTEC-6	XTec Incorporated	Rick Uhrig	G	12-13	609-687	2.9.1 & 2.9.2	This reiterates a point made by a workshop participant. The distinction between Renewal and Reissuance is unnecessary. The two can viewed as two aspects of the same use case. The following rules apply to the combined use case (Call it "Replacement"): - The Replacement PIV Card must be authorized by a proper authority if the expiration date extends beyond the expiration date of the PIV Card that is being replaced. - if the PIV Card being replaced is not collected and destroyed, then all digital certificates on the card must be revoked.	Consolidate "Renewal" and "Reissuance" into a single use caser called "Replacement." It is just as correct, yet cleaner and simpler.	Resolved by AMAG-11.
XTEC-7	XTec Incorporated	Rick Uhrig	T	14	672-673	2.9.5	The requirement "Any local databases that contain FASC-N or UUID values must be updated to reflect the change in status" is difficult and expensive to implement in its full generality. As a rule, the issuer will not be aware of the various relying parties that may have stored FASC-N or UUID values in local databases and has no mechanism for updating those databases. Even within the issuer's own organization, automatically updating LACS directories (e.g. Active Directory) or PACS head-ends is problematical, especially for large, distributed enterprises.	Reword the requirement to limit its scope to updating the issuer's local databases. Allow relying parties, and the issuer's own LACS and PACS to use OCSP and CRLs to validate their local databases.	Declined. Line 672-673 does not impose requirements on all relying systems.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
XTEC-8			T	15	715, 731	2.9.4	The language "matches the stored biometric on the [reset] PIV Card" suggests that the biometric must be matched to an instance stored on the PIV Card, and seems to exclude the most secure implementation, which is to perform the match at the IDMS/CMS with the corresponding biometric from the chain-of-trust. This method provides the most assurance and uses "issuer security controls equivalent to those applied during PIV Card reissuance" as required in line 695.	Use language that allows matching at the IDMS/CMS with the corresponding instance from the chain-of-trust, such as in lines 557-558: "matches the biometric available on the [reset] PIV Card"	Resolved by DoD-16, IL-4, and IL-5.
XTEC-9			T	15	730-731	2.9.4	Remote PIN Update should allow the biometric match that provides the most assurance and is most like the "issuer security controls equivalent to those applied during PIV Card reissuance."	Change the third bullet to read: "- the cardholder's biometric matches the biometric available on the PIV card through either a 1:1 biometric comparison at the IDMS/CMS or a 1:1 on-card biometric comparison."	Resolved by IL-5.
XTEC-10			E	26	1048		The information contained in the figures regarding font and size is important enough to be listed in he main text of the standard. Requirements should not be specified only in the captions of figures.	Add the following after line 1048: "All text is to be printed using the Arial font. Unless otherwise specified, the font size should be 5 pt. normal weight for data labels (also referred to as tags) and 6pt bold for actual data."	Declined. The figures are the appropriate place to define the default label and text font size requirements.
XTEC-11			E	27	1073	4.1.4.1	The table should show how to handle suffixes, e.g. "Jr.","III", etc	Provide an example	Declined. See Figure 4-2 for an example of a suffix.
XTEC-12	XTec Incorporated	Rick Uhrig	E	29	1106	4.1.4.2	The term "issuing facility" only occurs once in the standard. and "issuer's facility" occurs twice. These are not well-defined. There are at least 3 reasonable interpretations: (1) the location where the authority exists to issue the card, (2) the location where the card is printed, and (3) the location where the card is provided to the applicant	Clarify what the standard means by "issuing facility."	Declined. In Section 2.9.4 (now Section 2.9.3), the term "issuer's facility" may be any location that is maintained by the issuer, has the equipment necessary to reset the PINs on PIV Cards, and is staffed by someone to perform the PIN-reset procedure in accordance with the Standard and with local policy. In the description of the Issuer Identification Number in Section 4.1.4.2, the designation of issuing facilities is a department or agency prerogative
XTEC-13	XTec Incorporated	Rick Uhrig	E	30	1142		There are two expiration dates on the front of the card, Zone 14F and Zone 19F. The Phrase "above the expiration date" should be clarified	Replace the phrase with "above the Zone 14F expiration date"	Accept.
XTEC-14	XTec Incorporated	Rick Uhrig	T	44	1364		The requirement that, if present, the symmetric CAK "shall be unique" can only be enforced with absolute certainty if there is a registry across the entire PIV-issuing enterprise of all symmetric CAKs. That is unwieldy, undesirable and impractical. The point that the standard should be making is that agencies should not knowingly use the same symmetric CAK across multiple PIVs, but should instead be using diversification techniques to ensure a very high probability that symmetric CAKs will be unique. The same rules should apply for all symmetric keys -PIV Card Application Administration Keys and Symmetric CAKs	Replace with "shall be diversified to provide a very high probability of uniqueness."	Declined. The use of "shall be unique" for symmetric keys in FIPS 201-2 is consistent with its use in SP 800-57 Part 1 (Revision 3), and in neither place does it imply a requirement to compare each generated key with every other previously generated key to verify uniqueness. If cryptographic keys are generated in conformance with the relevant NIST recommendations, then uniqueness will be ensured.
XTEC-15	XTec Incorporated	Rick Uhrig	G	46	1426	4.2.3.2	Allowing On-card biometric comparison over the contactless interface provides convenience but also opens up a highly exploitable attack vector. It seems very wrong to force cardholders to carry cards with OCC against their will. These vectors would allow a card to be activated for authentication or digital signature without either a PIN being entered or the card being inserted into a card reader. How is a conscientious cardholder suppose to protect the PIV card from such attacks?	The standard should contain language requiring issuers to offer cardholders the option of opting out of OCC technology so that they can have higher assurance that their PIV card will not be activated without their consent.	Declined. Decisions about which optional features a card should support is a department/agency decision. The PIV Authentication and digital signature keys may only be used over the contact and virtual contact interfaces. The requirements for the virtual contact interface will be specified in SP 800-73-4. An initial draft of SP 800-73-4 was made available for public comment in May 2013.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
XTEC-16	XTec Incorporated	Rick Uhrig		47	1467-1468	4.3.2	The requirement that "each PIV Card shall contain a unique PIV Card Application Administration Key" can only be enforced with absolute certainty if there is a registry across the entire PIV-issuing enterprise of all PIV Card Application Administration Keys. That is unwieldy, undesirable and impractical. The point that the standard should be making is that agencies should not knowingly use the same symmetric PIV Card Application Administration Key across multiple PIVs, but should instead be using diversification techniques to ensure a very probability that they will be unique. The same rules should apply for all symmetric keys - PIV Card Application Administration Keys and Symmetric CAKs	Replace with "each PIV Card shall contain a diversified PIV Card Application Administration Key to provide a very high probability of uniqueness."	Resolved by XTEC-14.
XTEC-17	XTec Incorporated	Rick Uhrig	E	50	1567-1574	5.5	Recommend reordering three sentences for improved readability	Change to: CAs that issue authentication certificates shall maintain a Hypertext Transfer Protocol (HTTP) accessible web server that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it, as specified in [PROF]. In addition, every CA that issues these authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues. PIV Authentication certificates and Card Authentication certificates shall contain the crlDistributionPoints and authorityInfoAccess extensions needed to locate CRLs and the authoritative OCSP responder, respectively.	Resolved by DoD-46.
XTEC-18	XTec Incorporated	Rick Uhrig	T	54	1655	6.2.1	The statement that it "requires two interactions" is not necessarily correct. The card could be activated by OCC, obviating the need for a PIN	Change two: "May be a slower mechanism if two interactions with cardholder are required (i.e. PIN presentation and biometric} rather than just one (biometric for both off-card and OCC)	Resolved by PB-15.
XTEC-19	XTec Incorporated	Rick Uhrig	T	54	1662	6.2.1	Off-Card biometric comparison, in prior versions of FIPS 201, required 3 factors for authentication. Now it seems to require 2 or 3 factors, depending on whether PIN presentation or OCC is used to activate the card. This is worth noting.	Add bullet: It implements 2 or 3 factor authentication, depending on whether OCC (2 factor) or PIN presentation (3 factor) is used.	Declined See PB-15. Also, as noted in Table 7-1 of SP 800-116, BIO only provides one factor of authentication. While BIO requires the presentation of a card and a PIN in addition to the biometric sample, neither the card nor the PIN are authenticated as part of BIO, so they are not considered to be factors of authentication.
XTEC-20	XTec Incorporated	Rick Uhrig	T	54	1657-1658	6.2.1	Since OCC is now a possibility, the statement that the PIN is required is no longer true.	Change to "Strong resistance to use of unaltered card by non-owner since the cardholder biometric is required."	Resolved by PB-15.
XTEC-21	XTec Incorporated	Rick Uhrig	T	54	1660	6.2.1.1	Card can also be activated by OCC	Change to "The cardholder is prompted to submit a PIN or live biometric sample, activating the PIV Card."	Resolved by PB-15.
XTEC-22	XTec Incorporated	Rick Uhrig	T	55	1702	new	Tying together 3 different concepts within the standard - chain-of-trust, biometric re-authentication at re-issuance, and biometric authentication mechanisms - it is clear that "biometric authentication to the chain-of-trust" is a valid form of authentication that is required by the standard. It is also provides the highest level of biometric authentication available. As such, it should be explicitly recognized and allowed in Section 6 as an authentication mechanism.	Add a section for "Authentication Using the Chain-of-Trust Biometric."	Declined. Section 6 "defines a suite of authentication mechanisms that are supported by all the PIV Cards." Biometric authentication to the chain-of-trust does not involve use of the PIV Card, and so is out-of-scope for Section 6 of FIPS 201-2. Furthermore, while biometric authentication to the chain-of-trust may be an appropriate means of authenticating cardholders when performing card maintenance operations (e.g., issuance, reissuance, reset), it is not an appropriate general-purpose authentication mechanism due to access control restrictions that would need to be applied to the chain-of-trust maintained by each card issuer.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
XTEC-23	XTec Incorporated	Rick Uhrig	T	54	1673	6.2.1.1	May have already been performed for OCC	Add prefix, "If not previously provided, "	Resolved by PB-15.
XTEC-24	XTec Incorporated	Rick Uhrig	T	55-58	1699-1759	6.2.3 & 6.2.4	The authentication mechanisms that use challenge-response are written to a basic and inefficient implementation. Much more efficient implementations with equivalent or better security should be allowed, for instance: - reading the certificate at the time the PIV card is registered with the relying system, and associating the certificate with much shorter identifying number that can be read very quickly from the card. - performing certificate checks on the certificates registered with the system in the background, such as overnight, or whenever a new CRL is retrieved, so that the certificate status is already known.	Add a note to 6.2.3 and 6.2.4 allowing for alternate implementations with equivalent or better security. Specifically allow caching certificates, and performing certificate status checking as background task so that current certificate status information is at hand	Declined. FIPS 201-2 does not specify how to implement certificate checks as long as they are done. The proposed implementation details are already mentioned in SP 800-116.
XTEC-25	XTec Incorporated	Rick Uhrig	T	57	1740-1760	6.2.4	As the PIV Auth Cert or Card Auth Cert is available, the revocation status of the PIV card easily can be determined. While the description in 6.2.4 chose to omit revocation checking, that is not an inherent defect of SYM-CAK	Replace line 1757: "- Allows for but does not require revocation checking, does not provide protection against use of a revoked card when revocation checking is not performed."	Declined. While it is possible to perform revocation checking in combination with SYM-CAK, revocation checking is not a feature of SYM-CAK.
XTEC-26	XTec Incorporated	Rick Uhrig	E	60	1845-1848	6.3.1	There are two meanings of the word higher in play - "confidence" and "position in the table." The way the table is constructed, higher confidence means lower placement in the table. As a point of improved presentation, the table could be re-ordered so that higher confidence also meant the higher position in the table.		Declined. The term "higher" is used in the context of "higher assurance," and not to refer to "position in the table." This is consistent with SP 800-63-1.

List of Organizations

3M	3M
AMAG	AMAG Technology
AT	AssureTec Technologies
BAH	Booz Allen Hamilton
CB	Codebench Inc.
CDC	Centers for Disease Control & Prevention
CERT	CertiPath
DAON	Daon
DHS HQ	Department of Homeland Security HQ
DHS TWIC	Department of Homeland Security, Transportation Worker Identification Credential
DoD	Department of Defense
DOE	Department of Energy
DOE HQ	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOS	Department of State
EPA	Environmental Protection Agency
F	Factor 3 Technologies
FPKI	Federal PKI Policy
G	Gemalto
IBIA	International Biometrics & Identification Association
IL	Intercede Limited
NIH	National Institute of Health
OPM	Office of Personnel Management
ORC	Operational Research Consultant, Inc.
OSE	Open Security Exchange
OT	Oberthur Technologies
PB	Precise Biometrics
SCA	Smart Cad Alliance
SIA	Security Industry Association
SSA	Social Security Administration
TR	Department of the Treasury
TSCP	Transglobal Secure Collaboration Program
XTEC	Xtec Inc