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.advanceddetection.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
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.