Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AI-1	HID Global (ActivIdentity)	Dulude	E	2	274	1.3.3	Document defines and uses a new acronym OCC while industry uses the more common phrase "match on card" or MOC. In other places in the document the phrase "cardholder-to-card" or CTC is used (e.g., line 1795) is used.	Establish consistency within the document. Use industry standard MOC terminology.	Resolved by IBIA-1.
AI-2	HID Global (ActivIdentity)	LeSaint	G	8	477	2.4	There is a need for supplementary credentials bound to Secure Elements of mobile devices different than the PIV Card. This would leverage the authentication capabilities of mobile devices with non-smart card form factors, such as mobile phones. For instance this provision would allow email signing, or PKI logon from a mobile phone application relying on a secure element.	We recommend to leverage the existing FIPS 201 controls for Identity Proofing, Registration and Credential Issuance to allow supplementary credentials to be derived from the trusted enrolment package. For instance the issuer may require a 1:1 biometric match prior to equip a Secure Element (SE) with a PKI certificate. The SEs used as carriers for supplementary credentials may be subject to FIPS 140-2 policies. The supplementary credentials may be bound to the same PIV unique ID, and subject to similar usage policies as the PIV credentials, but would be distinct from the PIV credentials. The supplementary credentials may be independently revoked but their life cycle should be bound to the PIV card. i.e. when the PIV card is revoked all supplementary credentials are revoked. Their life should not exceed the PIV card life etc.. For instance supplementary credentials status and validity may be conditionned to the PIV card authentication credential status and validity.	Resolved by DOT-21. We plan to develop a special publication that addresses derived credentials consistent with SP 800-63-1.
AI-3	HID Global (ActivIdentity)	Dulude	E	13	643	2.5.6	The acronym "IIF" still appears	Replace with PII which is used in line 671	Accept use of PII. We will define PII with a reference to OMB M-07-16. Also, delete IIF from the glossary.
AI-4	HID Global (ActivIdentity)	Dulude	G	22	915	4.1.3	This sentence provides little value without examples	Remove sentence	Declined. We believe that it is useful to note that testing programs, such as FIPS 201 Evaluation Program, may perform additional testing; however, such testing is outside the scope of FIPS 201 and so examples cannot be provided.
AI-5	HID Global (ActivIdentity)	LeSaint	T	37	1139	4.1.6.1	The Card management key should also be an Asymmetric key. Authentication protocols with session key establishment based on Asymmetric keys offer desirable confidentiality properties. For instance , with certain asymmetric key protocols, after a key transport session ends, the knowledge of the management key cannot be used to reveal the transported key. This is not true with symmetric keys.	Allow asymmetric key card management keys.	Out of scope - The Card Management key is the PIV Card Application Administration key used to manage the PIV card application, and it is only used for authentication. Keys used to establish secure session for card management are outside the PIV card application and therefore are out of scope for FIPS 201. Replace all occurrences of 'Card Management Key' and associated certificate with "PIV Card Application Administration Key."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AI-6	HID Global (ActivIdentity)	LeSaint	T	38	1174	4.1.7.2	When secure messaging is used to perform card management operations, (e.g. SCP03), a PIV card needs a management key set composed of several management keys. The value of each key of the key set must be globally unique.	replace with "each PIV card is exclusively bound to one or several globally unique card management keys"	Resolved by AI-5.
AI-7	HID Global (ActivIdentity)	LeSaint	T	39	1231	4.3	Once a secure messaging session with card authentication has been set through the contactless interface, (for instance with Opacity ZKM) it should be possible to input the PIN or OCC thorugh that secure channel. After the PIN or Biometric has been verified, the channel is trusted on both sides, and could be used for performing cryptographic operations or reading PIV data elements. This would for instance allow 2- or 3-factor contactless authentication operations. For card management or remote authentication it is desirable to use a mutually authenticated channel. (for instance Opacity Forward secrecy) More generally the protection of PIV card commands with secure messaging obtain from either card authentication or mutual authentication should be possible in contactless or wireless situations.	replace with "the cryptographic private key operations shall be performed only through the contact interface unless they are protected with secure messaging established with appropriate authentication level".	Resolved by stating that once secure messaging has been established, a virtual contact interface may be established and by stating that cryptographic private key operations (and any other operations that may be performed over the contact interface) may be performed over either the contact interface or the virtual contact interface.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AI-8	HID Global (ActivIdentity)	LeSaint	T	41	1282	4.3	When the Asymmetric Card Authentication key is an on card generated elliptic curve key pair, it may also be associated with a card verifiable certificate (CVC) as described in ISO 7816-8 Annex B. A CVC with Elliptic Curve cryptography can be extremely compact (150-180 bytes for P-256) and allows for rapid PKI authentication through contact or contactless interfaces. This may greatly enhance the user experience for PKI authentication at the door. And simplifies key management. A CVC cryptographically binds a EC public key generated on card with a unique PIV card idenitifier. The CVC is signed by the PIV card issuer using a unique CVC signing key pair. The binding bewteen the issuer and CVC signing verification public key should itself signed by a digital signatory (PIV signer Dn), thus forming a trust chain. The resulting signed object does not need to be stored on the PIV card but it allows relying parties such as Physical Access Control systems to register CVC verification keys and periodically check their status. CVC are not actual certificates, but their status status maybe confounded the Card Authentication key certificate. The above arrangement allows the deployment of CVC-based protocols such as Opacity ZKM and Opacity FS in GICS, and thereby great gains in speed, with the opportunity to secure the contatcless interface with secure messaging..	Mention the optional addition of a Card Verifiable certificate to the Card Authentication key certification data.	Declined. A new key will be created for establishing secure sessions. If the option to use CVC is introduced, it will be for the key(s) specific to establishing secure sessions. Further details will be specified in SP 800-73-X.
AI-9	HID Global (ActivIdentity)	LeSaint	T	42	1313	4.1.7.2	When secure messaging is used to perform card management operations, (e.g. SCP03), a PIV card needs a management key set composed of several management keys.	Replace with: ".. The card management key(s)..."	Declined - see AI-5.
AI-10	HID Global (ActivIdentity)	Dulude	T	49	1573	5.5.1	The popularity of the http protocol to retrieve PKI related data has resulted in the LDAP protocol being seldom used and of little practical value. The LDAP protocol has already been deprecated in the PIV-I specs.	Require http protocol only throughout the document and delete LDAP requirement.	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AI-11	HID Global (ActivIdentity)	Dulude	T	50	1582	5.5.2	HSPD-12 identifies interoperability as a primary goal for the PIV program. The Federal Bridge was implemented to enable interoperability of these PIV cards for PACS and LACS authentication. No where however is there a requirement for SCVP responders to enable the rapid electronic authentication (line 353) goal. This seems to be a glaring oversight.	Add a section stating that SCVP responders shall be implemented … Note that most SCVP responders support both SCVP and OCSP and may be able to use the same URI.	Declined. An OCSP responder may either be operated on behalf of the relying party (a locally-trusted OCSP responder) or by (or on behalf of) the CA. In FIPS 201-2, references to OCSP are only for OCSP responders operated by (or on behalf of) the CA. An SCVP server can only be operated on behalf of the relying party. While we do not discourage the deployment and use of SCVP, it is out-of-scope for FIPS 201-2.
AI-12	HID Global (ActivIdentity)	Dulude	T	61	1624	A.5	There has been major confusion in the industry regarding the FIPS 201 Evaluation Program over the difference between approved "readers" and "approved authentication systems".	Address this confusion by explicitly indicating here where each approval applies. Specifically when and where approved authentication systems are required.	Out of scope - Applicability and implementation planning are out of scope for FIPS 201. The Appendix indicates areas of testing and responsible parties. Complete details of test categories, approval procedures, and test procedures are provided and maintained on the FIPS 201 Evaluation Program website by GSA.
AI-13	HID Global (ActivIdentity)	LeSaint	T	54	1718	6.2.3	Contacless readers should be authorized to access the PIN-protected biometric information. For instance, the following sequence is proposed: - open secure channel using Opacity ZKM (PKI card authentication). Set response confidentiality for secure messaging. - Verify PIN through the same secure channel. If successful, the PIV card allows reading biometric information through that channel in confidential (encrypted mode) only. - Get Biometric information through the same channel, encrypted. Once the PIN has been validated through the channel, it means that the other end of the channel is a process trusted by the user. Sensitive data can be safely transmitted encrypted through the contactless interface.	Allow access to PIN-protected biometrics I18	Resolved by AI-7.
AI-14	HID Global (ActivIdentity)	Dulude	T	55	1730	6.2.3.1	Because of the use of a "shall" in line 1720 of this section it implies in line 1730 that the CHUID must be read to retrieve the FASC-N for the comparison check with the FASC-N in the signed biometric data block. Alternatively the FASC-N could be read from the PIV Auth certificate and compared with the FASC-N in the signed biometric data block. There are two advantages to this approach: 1) the PIV auth cert can be tied to the card via a challenge response making it more secure (note both the CHUID and Biometric data block can be copied), and 2) using the CHUID for this process could require reading the full CHUID to check its signature which will significantly increase the processing time and degrade performance. In either case the most likely implementation would have cached the signing certificate.	Since these are presumably examples and not normative prescriptions for how the various authentication mechanisms could be implemented the "shall" in 6.2.3.1 and 6.2.3.2 should be removed.	Resolved by allowing option to use other data elements.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AI-15	HID Global (ActivIdentity)	Dulude	E	55	1732	6.2.3.1	In many places in the document the phrase "unique identifier" is used to describe the input to the authorization process (e.g., lines 1695, 1769 and 1814). However, in other places the term FASC-N is used for the same purpose (e.g., line 1732, 1748,1786, etc.)	Used the phrase "unique identifier" everywhere for consistency within the document and with the PIV-I specifications as well as in anticipation of future changes within PIV.	Resolved by NIST -81.
AI-16		Dulude	T	56	1769	6.2.4.1	The Subject Distinguished Name (DN) is typically not required in the implementation of this authentiation process. Only the unique identifier is needed.	Remove the reference to Subject Distinguished Name (DN) to eliminate confusion.	Resolved by NIST-81.
AI-17	HID Global (ActivIdentity)	Dulude	T	56	1772	6.2.4.1	The use of the phrase "online" certificate status checking infrastructure in the first version of this document caused considerable confusion within the industry as many people interpreted this to mean for use in "real time" revocation checking. In fact there must be a certificate status checking infrastructure but it does not have to be "online" at the time the revocation checking is done. The data can infact be cached.	remove the word "online" from this sentence. The word "infrastructure" says what needs to be said.	Accept to remove the word 'online'.
AI-18	HID Global (ActivIdentity)	LeSaint	T	56	1775	6.2.4.1	Contacless readers should be authorized to perform PKI-AUTH if the transfer is protected with secure messaging with response confidentiality obtained after session key agreement with PKI card authentication and PIN verification thorugh secure messaging. (eg. Opacity ZKM) See rationale above (AI 13)	Allow PKI-AUTHfrom the contactless interface using a PKI secure channel with card authentication only.	Resolved by AI-7.
AI-19	HID Global (ActivIdentity)	Dulude	T	56	1789	6.2.4.2	same comment as above for line 1772		Accept to remove the word 'online'.
AI-20	HID Global (ActivIdentity)	Dulude	T	49	1560+	5.5	It appears that to revoke a card that both the PIV auth and Card auth certificates need to be revoked. However, either (but not both) auth certificate can be revoked without the card being revoked. See continuation of this comment below (for line 1643)		Resolved by AI-21.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AI-21	HID Global (ActivIdentity)	Dulude	T	52	1643+	6.2	In this section it states that the status of the auth certificates is directly tied to the status of all other credential elements held by the card. This raises the question of the status of these other elements if only one auth certificate is revoked. (View this comment in conjunction with the above comment for line 1560+)	Clarify the status of the other credential elements held by the card if only one authentiation certificate is revoked. This is critical for correct authentication processing at the relying party.	Declined. Both the PIV Authentication certificate and the Card Authentication certificate are mandatory in Draft FIPS 201-2, and so a valid PIV Card is required to have both a valid PIV Authentication certificate and a valid Card Authentication certificate. If a card is still valid, but one of the authentication certificates is revoked then that authentication certificate must be replaced with a valid certificate. In the (very unlikely) event that one of the authentication certificates has been revoked and the other hasn't, and the revoked certificate has not yet been replaced, the PKI-AUTH and PKI-CAK authentication mechanisms will yield different results. However, this is unavoidable, and we would not recommend that relying parties perform both authentication mechanisms (which would not always be possible) just to verify that both authentication mechanisms yield the same result.
AI-22	HID Global (ActivIdentity)	Hoyer	E	52	1626	6.1.1	The table states relatioinship between PIV and OMB-04-04 E-Authentication levels but the content shows the realtionship between OMB-04-04 E-Auithentication levels and PIV	Reverse the table and pout PIV levels fist on the left	Accept.
AI-23	HID Global (ActivIdentity)	Hoyer	T	55	1730	6.2.3.1	If CHUID is used and after step 8 there is not a specific need to restrict the access authrozation to be based on FASC-N. One can base the access authorzation similar to the Section 6.2.2 step 4: "A unique identifier within the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access."	Change step 9 to: "A unique identifier within the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access."	Resolved by NIST-81.
AI-24	HID Global (ActivIdentity)	Hoyer	T	55	1730	6.2.3.2	Same as coment above for Step 9	Change step 9 to: "A unique identifier within the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access."	Resolved by NIST-81.
AI-25	HID Global (ActivIdentity)	Hoyer	G	53	1666+	6.2.1 and 4.4.1	It would be very beneficial to define a seperate electronic secure VIS authentication whereby the cardholder hands the card to a guard or inserts it into a reader and the facial image is displayed on a secure viewer after having read the CHUID and checked its validity. This is also referenced in section 4.4.1 line 1387.	Add a new Visual authentication mechanism	Declined. The proposed solution imposes an extra burden to require PIN pad and contact reader to extract the facial image from the card. Alternate method to retrieve facial image and display on the screen from the back-end system might be a better approach.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AMAG-1	AMAG Technology	Adam Shane	G			1.3.1, pg. 2	There is no such thing as a backward compatible change in a standard. The example given seems benign in that a previously mandatory field becomes optional. This would be backward compatible to a card issuance system, but is not backward compatible to an authentication system that relied on that information being present. Conversely, if a field changes from optional to mandatory it may be a burden on the issuance system but not on the authentication system.	Strike section 1.3.1. Add the following to section 1.3.2. Any change to the standard will have significant and sometimes costly impact on fielded solutions.While some changes may impact PIV issuers and not PIV authenticators, other changes may impact PIV authenticators and not issuers, and other changes may impact both. Correct all references to backward compatible change in the document to indicate Non-Backward Compatible Change.	Declined. We explain in Section 1.3.1 what a backward compatible change is (from the viewpoint of the system that uses existing features). Declined: Out of scope. FIPS 201-2 revision has been written with both impact and costs in mind. Declined as explained in the first line of this response.
AMAG-2	AMAG Technology	Adam Shane	G			1.3.4, pg. 2	Depricated features are non-backward compatible changes to the standard. The depricated field/feature becomes optional. This would be backward compatible to a card issuance system, but is not backward compatible to an authentication system that relied on that information being present.	Add the following to section 1.3.3. Any change to the standard will have significant and sometimes costly impact on fielded solutions.While some changes may impact PIV issuers and not PIV authenticators, other changes may impact PIV authenticators and not issuers, and other changes may impact both.	Declined. FIPS 201-2 has been written with both impact and costs in mind. See also AMAG-1.
AMAG-3	AMAG Technology	Adam Shane	T			2.3, pg 6	Department of Defense Common Access Card is a PIV card and therefore, if someone has possession of such a card, they should not have to be subjected to a secondary issuance process. This is equivalent of including "PIV card issued by another agency" in this list, which ignores the interoperability premise of the program.	Remove reference to DOD CAC as an identification document in section 2.3.	Resolved by replacing the Common Access Card with the PIV Card on the list. Note: The chain-of-trust mechanism will eliminate the need to repeat the complete registration and issuance process (see DOT-10).
AMAG-4	AMAG Technology	Adam Shane	E			2.5.1, pg 9	"The cardholder will not be allowed to starrt the renewal process if the original PIV card is expired."	This should be left to the discretion of the agency. It seems wasteful to have to restart the entire issuance process if the person is a day or a few weeks beyond the expiration date compared to a day or a few weeks prior.	Declined. Considering the efficiencies gained with chain-of-trust and relocating NACI, the identity proofing and registration process is much less onerous.
AMAG-5	AMAG Technology	Adam Shane	T			2.5.6, pg 12	Section 2.5.6 does not include a time frame in which the certificates should be revoked. Furthermore, a statement should be included that standard pocessing times are not acceptable in the case of life safety and other exigent circumstances. Therefore an expedited time frames should be included.	Statement should be added that, "Just as in section 2.5.2, the card validation certificates and signature signing certificates must be revoked. Every effort should be made to accomplish this within 18 hours. In exigent circumstatnces such as life safety or other threat to safety or properly, 18 hours may not be acceptable. Every effort should be made to follow described procedures."	Resolved by changing the bullet item in Section 2.5.6 (now Section 2.9.5) to say "The PIV Card shall collected and destroyed, if possible." and by adding the following text after the bulleted list: "If the card cannot be collected, normal termination procedures shall be completed within 18 hours of notification. In certain cases, 18 hours is an unacceptable delay and in those cases emergency procedures must be executed to disseminate the information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AMAG-6	AMAG Technology	Adam Shane	G			4.1.6, pg 36	Section 4.1 is Physical PIV Card Characteristics. 4.1.6 is a sub-section of 4.1 and describes Logical Credentials which are, nearly by definition, not physical characteristics of the card.	4.1.6 and subsections should be moved to Section 4.2 with a new title, "Logical/Electronic PIV Card Credentials". Current section 4.2 "CHUID" is actually a subsection of Logical Credentials.	Resolved by revising the sections as follows: 2.2 Credentialing Requirements 2.3 Biometric Data Collection for Background Investigations 2.4 Biometric Data Collection for PIV Card 2.5 Biometric Data Use 2.6 Chain-of-Trust 2.7 PIV Identity Proofing and Registration Requirements ...Rest of the sections have been renumbered accordingly 4. PIV Front-End Subsystem 4.1 PIV Card Physical Characteristics 4.1.1 Printed Material 4.1.2 Tamper Proofing and Resistance 4.1.3 Physically Characteristics and Durability 4.1.4 Visual Card Topography 4.1.4.1 Mandatory Items on the Front of the PIV Card 4.1.4.2 Mandatory Items on the Back of the PIV Card 4.1.4.3 Optional Items on the Front of the PIV Card 4.1.4.4 Optional Items on the Back of the PIV Card 4.1.5 Color Representation 4.2 PIV Card Logical Characteristics 4.2.1 Cardholder Unique Identifier (CHUID) 4.2.2 Cryptographic Specifications 4.2.3 PIV Biometric Data Specifications 4.2.3.1 Biometric Data Representation 4.2.3.2 Biometric Data Protection 4.2.3.3 Biometric Data Access 4.2.4 PIV Unique Identifiers 4.3 PIV Card Activation 4.3.1 Activation by Cardholder 4.3.2 Activation by Card Management System 4.4 Card Reader Requirements 4.4.1 Contact Reader Requirements 4.4.2 Contactless Reader Requirements 4.4.3 Reader Resilience and Flexibility 4.4.4 Card Activation Device Requirements
AMAG-7	AMAG Technology	Adam Shane	G			4.1.7, pg 37	Section 4.1 is Physical PIV Card Characteristics. 4.1.7 is a sub-section of 4.1 and describes PIV Card Activation which has nothing to do with Physical characteristics of the PIV Card..	A new section should be created for Activation.	Resolved by AMAG-6.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AMAG-8	AMAG Technology	Adam Shane	T			4.1.3, pg 21	The antenna interconnect to the ICC is the most common failure mode of the PIV cards. However, this isn't addressed in FIPS 201 as it should.	Add additional requirements in 4.1.3 such that the antenna shall not become disconnected from the ICC during the environmental exposures indicated. Additionally, heating to 160-180 degrees C during the printing/laminating process has been shown to exascerbate this issue and should be specificially included in the environmental exposure testing.	Declined. The standard already requires durability and environmental testing as specified in national and international standards for smart cards.
AMAG-9	AMAG Technology	Adam Shane	T			4.2, pg 38	The statement that a CHUID should be treated as if it were a password is inappropriate and inaccruate. CHUID is an identifier and not a password. Just as many systems use an email address as an identifier and a password to log in to an account, only the password is treated as a password. If the CHUID is treated like a password, then it cannot be used as an effective identifier. Possession of the CHUID does not even represent a single trusted factor for authentication, and therefore poses little threat if it is exposed.	NIST should remove the statement discouraging storage of the CHUID. NIST should indicate that CHUID, and other PII data should be encrypted at rest as well as in transit.	Resolved by removing the third paragraph of Section 4.2 (now Section 4.2.1), lines 1184-1187. Decline to indicate that PII data should be encrypted since it is already covered by FISMA.
AMAG-10	AMAG Technology	Adam Shane	E			4.5.2, pg 46	The word "contact" is used in the paragraph referencing contactless card readers.	Change the word to "contactless"	Accept.
AMAG-11	AMAG Technology	Adam Shane	T			6.3, pg 58	NIST ignores the common sense recognition that there is a spectrum of strength across all authentication factors. A visual inspection can be done by someone with good eyesite or poor, trained or not trainied. Biometrics can be as simple as checking but a few minutia points to much more robust solutions. Card possession with or without PKI also represent various degrees of single factor authentication.	NIST should elaborate on the appropriateness of various authentication mechanisms in light of their relative strength. NIST should clarify that not all mechanisms for providing authentication factors are created equal and therefore should be judged on their strength as well as providing the additional factor of authentication.	Noted. The authentication methods listed in Tables 6-2 and 6-3 are aligned with OMB M-04-04.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AUDoD-00	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	G			NA - Background	Australian Department of Defence (AUDoD) has an interest in FIPS-201 due to both defense and civil security related treaties, agreements and day-to-day operations involving Australia, the US and our joint allies. Interoperability with the US DoD has become a mission critical requirement for the AUDoD and compliance with technical elements of FIPS-201-2 and related NIST technical specifications is therefore essential in achieving compatible identity authentication to support interoperability and information exchange outcomes. AUDoD is currently implementing a strategy which will technically align the merged US Common Access Card (CAC)/PIV programs, and enable cross certification of PKI-based authentication mechanisms supporting card schemes under existing or new agreements and treaties. NISTs revision of FIPS-201-2 and consideration of the issues raised in this response is therefore greatly appreciated since it will assist in assuring interoperability in our joint forward critical infrastructure.	Much of FIPS-201 is related to very specific US policy issues - This AUDoD response does NOT seek to make comment on these issues. In the Australian context they are replaced by local policy under our local IMAGE (Identity Management for Australian Government Employees) program. We do provide a number of technical contributions which relate either directly to FIPS-201-2 and/or to referenced NIST documents. (I.e. specifications which will require review consequent to this update of FIPS-201.) These follow as comments AUDoD-01 to AUDoD-14	Noted.
AUDoD-01	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	G			NA - Technical Policy	AUDoD notes that the operational use cases for PIV/CAC cards require both contact and contactless capability, and that in many cases contactless usage may be the only practical interface, particularly in military applications where dirt, dust and grease may prevent contact operations. In many cases contactless use for Logical Access Control Systems (LACS) (even in office environments) may be more suitable, since it enables "no-de-badging" rules to be applied and discourages cards being left behind in readers with consequent poor security results. The way FIPS-201 is currently designed, the contactless interface is considered to be the inferior interface, and restrictions are placed on it. AUDoD considers that most of these restrictions are design restrictions related to limitations generated from the design of the authentication protocols currently in use under FIPS-201, and not with the actual interfaces themselves. It is AUDoD's view that with suitable authentication protocol improvements, these restrictions should be able to be deprecated, and this will improve the utility, functionality and business case for PIV deployment. This will also impact forward options related to authentication using alternate (non-card) form-factors, where the same principal of interface neutrality might usefully be applied. More detailed suggestions are made in relation to specific authentication protocols in subsequent contribution in this response.	Consider a strategy to improve authentication protocol design so as to eliminate restrictions on the use of contact versus contactless interfaces and/or differences due to alternate non-card form factors with an end target that all authentication protocols in use by FIPS-201-2 can operate equally over any interface or form factor. This comment does not apply to administrative interfaces where physical capture of the card during administrative update is a clear security requirement. This comment does not apply to visual (VIS).	Resolved by AI-7.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AUDoD-02	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	G			NA - Technical Policy	AUDoD notes that a significant amount of uniquely identifiable data is available in the clear in the Card Holder Unique IDentifier (CHUID) structure. This data could be used, at a minimum, to assist an attacker in determining disposition of forces, and potentially to assist a range of other attacks. Availability of the readily identifiable data can create a false expectation of security, particularly in Physical Access Control System (PACS) implementations. AUDoD does not therefore intend to populate the CHUID structure, and can't currently identify any use-cases where it is in fact required. NIST should note that the CHUID structure is therefore not a data element over which we see any requirement for interoperability with US forces or agencies. AUDoD do not intend to build systems which rely on this structure	Consider long term deprecation of the CHUID structure in favour of specific authentication protocols which evaluate appropriately for the designed range of use-cases. This might also minimise or eliminate the need for shielding of PIV/CAC cards when not in use. Advise relying parties that international interoperability is not possible using the CHUID data structure. Accelerate the support for RFC 4122 based Universally Unique IDentifier (UUID) so as to be available from all supported authentication protocols (and certificates) under FIPS-201-2 .	CHUID structure will not be deprecated to maintain backward compatibility with existing implementations. CHUID authentication mechanism will be deprecated. International interoperability is outside the scope of HSPD-12. UUID will be made mandatory per DoD-41.
AUDoD-03	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	G and T			NA - Technical Policy	AUDoD notes that there are inconsistencies in the intent of FIPS-201-2 draft versus the requirements of FIPS 140-2/3. This FIPS 201-2 draft includes important policy changes which facilitate post-issuance update of PIV cards, which are supported. However the cryptographic module requirements of FIPS 140-2/3 are still interpreted as preventing post-issuance update or the addition of other applications to PIV/CAC cards without re-accreditation. These restrictions reduce efficiency and prevent stronger business cases being developed for little or no real gain in regard to security, since security architectures are already in place under GlobalPlatform which address application load related security issues.	Consider the architectural separation of security domains within FIPS-201-2 so as to separate the accreditation of FIPS-201 applications from the GlobalPlatform application load environment and/or Card Operating System (COS) and/or ICC hardware such that FIPS-140-2/3 accreditation applies to the latter and FIPS-201 applies to the former. Consider separating the accreditation of both PIV and other applications (if any) which an agency might load to an accredited FIPS-140-2/3 core hardware/COS/GlobalPlatform environment so as to enable broader business cases than purely PIV without generating high accreditation costs for those implementations.	Declined. FIPS 201 Post issuance update refers to PIV Card data object updates and not new application loading. It is outside the scope for FIPS 201 since this is an issue of implementation and CMVP requirements.
AUDoD-04	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	G and T	40	1263-1264	NA - Policy	FIPS-201-2 draft significantly improves the functionality of the contactless interface, which is supported. However, performance related boot self-check restrictions generated out of FIPS-140-2/3 mean that the new capability may not be able to be efficiently utilised. The boot self-check on most current generation cards takes between 200-400ms and is generally longer than typical contactless PACS authentication protocol transactions on the same integrated circuit chips (ICC). This results in frequent transaction "tears" on the subsequent authentication and a poor cardholder experience.	Consider clarifying the FIPS-140-2/3 requirement for cryptographic modules when implemented as ICCs to do a cryptographic self-check at every boot cycle by reducing this requirement to only perform a self-check "on command". This will make FIPS-201-2 significantly more functional for contactless interfaces (where speed is of the essence). Along with this change consider adding a requirement for administrative interfaces to verify the self-check before any administrative operation, so that at the critical time a self-check is required (before administrative access) such an operation is performed and administrative access should be contingent on a self-check pass.	Declined. It is outside the scope for FIPS 201 since this is a CMVP requirement.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AUDoD-05	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	T	14	693-694	2.6	It is unlikely that a protective sleeve or any other technology can fully protect against the reading of a CHUID (or any other on-card data) held in the clear, whether it be a contact or contactless interface. For a contact interface it is arguably easier since you may convince end-users to insert their cards into un-accredited laptops or systems by various ingenious ruses. For a contactless system it is possible to read a CHUID transaction whenever a card is in use, and most people will present a card to a person who appears to have some authority and requests it in any case, irrespective of whether they have appropriate authority or not. Further - consider that 13.56mhz readers are available which have been up-rated to generate much stronger fields and therefore longer reading ranges - up to 200mm. The power of these devices will circumvent some existing shielding technologies and make directed attacks possible.	Delete sentence and; Consider discussion in AUDoD-01 , AUDoD-02 and AUDoD-07 as a solution rather than relying on countermeasures which rely on human intervention. Consider gradual deprecation of authentication protocols which are weak (particularly involving free read structures such as CHUID) in regard to privacy.	Decline specific request. Mutual authentication is not feasible across agencies, and it is not backwards compatible. We will update the sentence about the protective sleeve to "Specifically, employees may choose to use…."
AUDoD-06	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	G and T	37 and 38 but many other related references	1139, 1169-1176	4.1.6.1 and 4.1.7.2 and many other usages need clarification	Discussion in FIPS-201 related to "card management" uses the single term "card management system". However, in many cases the actual entity being managed is the "on-card application", not the ICC hardware or the on-card ICC card management security domain. This results in some potential confusion, and this paragraph is a good example, where the dot-point at line number 1139 "A symmetric key associated with the card management system" could be interpreted in two ways; - A) as a GlobalPlatform key for securing the application load of the PIV application or, - B) as an administrative key for management of the PIV application (AUDoD expects this to be the intended interpretation) Paragraph 4.1.7.2 is a further example of this confusion, where the first and second sentence most probably refers to A) above, but the rest of the paragraph most probably refers to B) . (We are not clear). Note that this issue has also caused legal confusion in relation to export licence controls under the US Export Administration Regulations for card and card applications and their cryptographic linkage to card management systems supporting PIV.	Suggest that language used through FIPS-201-2 should differentiate between the "Card Management System", being the system which manages the card application load and related security domain/s under GlobalPlatform and the "Card Application Management System" or "PIV Application Management System" being the administrative system which is used to secure, configure and provision the PIV application on the card. This also makes it much clearer when other (non-PIV) applications are managed on the card.	All references to card management system in FIPS 201 refer to PIV application management. Resolved by adding definition of card management system to glossary.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AUDoD-07	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	G and T	38, 39	1177-1224	4.2	Refer AUDoD-01 to 03 and AUDoD-05. AUDoD intends to implement the AS-5185 PLAID authentication protocol in order to resolve the authentication protocol strength, privacy and cloneability issues of the CHUID. PLAID can be used by PACS to deliver a Federal Agency Smart Credential - Number (FASC-N), RFC 4122 UUID or older Weigand records privately and securely whilst operating in the 200-400ms transaction time range. AS-5185 PLAID is also being fast tracked to an ISO standard as well as being available to any implementer for free from the Australian Commonwealth. It is also under consideration by ANSII-INCITS GICS. We recommend implementation as a separate Application IDentifier (AID) and security domain to PIV, and this makes implementation quite simple and independent. AUDoD is able to support PACS interoperability with US forces via CAC using shared operational key sets under PLAID on any existing PIV or CAC card subject to post-issuance update and 10kb free memory.	Consider gradual deprecation of CHUID in favour of AS-5185-PLAID (and its forward ISO version) as a separate AID to PIV with the CHUID being deprecated by not being populated in the first deprecation instance. Move FASC-N to being one of at least three objects supported under PLAID, these being FASC-N, RFC 4122 UUID, and one or more Weigand records (agency dependant) for use during transition from existing PACS systems. Note that we expect the longer term target credential record being support by all parties will be RFC 4122 UUID. Note that we expect to support PKI-CAK for PACS in the longer term (5-10 year period) but it will be at least 5 years before commercial product at a commercial price-point will be available. We can support AS-5185 PLAID now with much less infrastructure change and cost.	Declined. Mutual authentication is not feasible across agencies, and it is not backwards compatible.
AUDoD-08	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	T	41 and 57	1293-1298 and 1802-1815	4.3, 6.2.6	A positive improvement in FIPS-201-2 is the ability to potentially use symmetric ciphers in authentication protocols requiring speed, such as PACS protocols (including PLAID). However neither this draft nor the current draft of Special Publication (SP) 800-78 or SP-800-73 provide either informative guidance or normative specifications for key diversification methodologies that should be utilised to protect the exposure of master keys through the exposure of a single card or readers keys. Because this is not specified, at best, it is likely that implementations will end up utilising proprietary methods, and interoperability will not be achieved between different implementations. At worst agencies may choose to implement with no key diversification (common in current PACS systems supporting symmetric ciphers) and the end result is that master keys, once exposed, require the re-issuance or re-key of every ICC in the systems breached.	Suggest the documentation of key diversification as a normative requirement for all symmetric cipher based authentication protocols. Suggest that generic PACS protocols should be explicitly specified so as to enable interoperability, in particular AS 5185-PLAID could be specified to fully resolve this requirement for PACS (refer AUDoD-07). Note that AS 5185-PLAID provides a normative method for key diversification for PACS which may be freely utilised by NIST.	Resolved by IDTP-28. Declined. Specific protocol will be specified in SP 800-73. Noted.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AUDoD-09	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	G and T			NA - Technical Policy	It is fairly clear that most recent successful attacks on ICCs and related systems have been against the authentication protocol rather than the cryptographic cipher. This trend is likely to continue, since the ciphers are rigorously evaluated and gradually improved, whereas the current methodologies to evaluate authentication protocols are significantly less rigorous in regard to specification, evaluation, implementation, certification and system accreditation. ISO/IEC 24727-3 makes a start at separating the Authentication Protocol from the Cipher, and the announced use of ISO/IEC 24727 methodology in FIPS-201-2 is supported. It may be possible however, even under this version of FIPS-201-2 to start to separate out the various authentication protocols which are evaluated as fit for particular purposes, and start to set up infrastructure which might support a more rigorous specification and accreditation of authentication protocols in SP-800-73 etc.	Consider defining Authentication Protocols within FIPS-201-2 using the ISO/IEC 24727-3 and related Part 6 methodologies so that references to deprecated and new authentication protocols can be modular over time, making it much easier to wind in and out different technologies as they might be broken. FIPS-201-2 might for instance link assurance levels at 6.3 to specific authentication protocols called out in SP-800-73.	Noted: The PIV Card Application uses only a small subset of Authentication Protocol defined in ISO/IEC 24727. For agencies planning to introduce ISO/IEC 24727 capabilities, a profile will be introduced after proof-of-concept and after OMB guidance.
AUDoD-10	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	T	57	1701 to 1815	6.2.3, 6.2.4, 6.2.5 and 6.2.6	Authentication mechanisms as described rely on the FASC-N and do not support RFC 4122 UUID. Consequently they are not interoperable beyond pure US federal agency usage under PIV, in spite of the fact that SP-800-73 describes PIV-I and UUID interoperability based on both.	Describe authentication mechanism interoperability for both FASC-N and UUID based credential use cases, and preferably signal deprecation of FASC-N in the longer term. Consider adding AS-5185-PLAID authentication as a PIV-PACS method which can support all of FASC-N, UUID, as well as multiple Weigand 26-80 Bit as well as pre or post authentication PIN as well as off-card biometric (BIO) authentication.	Resolved by NIST-81. PLAID is not feasible across agencies, and it is not backwards compatible.
AUDoD-11	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	T	40,41	1267 to 1292	4.3	Authentication keys and related X.509 certificates rely on FASC-N and do not support RFC 4122 UUID. Consequently they are not interoperable beyond pure US Federal agency usage under PIV, in spite of the fact that SP-800-73 describes PIV-I and UUID interoperability based on both.	Describe authentication key and related X.509 certificate interoperability for both FASC-N and UUID based credential use cases, and preferably signal deprecation of FASC-N in the longer term.	Resolved making the UUID mandatory as per NIST-81 and DoD-41. No plans for deprecating FASC-N.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
AUDoD-12	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	E	40,41	1267 to 1315	4.3 (move to 5.2.1)	Section on key management includes significant discussion on X.509 certificates which is repeated later in document - This generates confusion on which requirements take precedence	Move and merge content related to X.509 certificate contents to section 5.2.1	Declined - Both sections are required - Section 4.3 (now Section 4.2.2) is more specific to the PIV card cryptographic keys while Section 5.2.1 is more specific is more specific to the key management structure/requirements.
AUDoD-13	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	E	57	1799, 1800, 1801	6.2.5	Editorial only	Missing "the" before "department" Typo - word "alf" should be "if"	Accept.
AUDoD-14	Australian Department of Defence (AUDoD)	Identity.Management@defence.gov.au; graeme.freedman@defence.gov.au; michael.cole5@defence.gov.au	E	13	660	2.6	Editorial only. Deletion of words from the previous version has affected the grammatical 'flow' between line 660 and subsequent sub-paragraphs	Consider adding 'departments and agencies shall do the following" after 'PIV life-cycle'	Accept.
B&W-1	B&W Y12 National Security Complex	Steve Macklin	G			G.	Is there a requirement to retrieve the HSPD-12 badge when the certificates on the PIV chip have expired even though the card has not expired? If so, what is the requirement?		Card termination requirement is defined in Section 2.5.6 (now Section 2.9.5).

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Bell-1	Bell ID	Lex Meijer				General	The new chain-of-trust is applicable for both renewal and reissuance processes of a PIV card and it actually makes these processes less different. In both scenario's the old card is collected/surrendered (if no lost) and terminated/revoked. Why is FIPS201 continuing to distinguish renewal and reissuance processes and not define a single PIV Card Replacement process?		Declined. The two processes are indeed different and serve different purposes.
CDC-1	CDC	Cherri Gatland-Lightner	G				CDC has no comments regarding the *DRAFT FIPS 201-2, Personal Identity Verification of Federal Employees and Contractors.* Thank you for the opportunity to review and comment.		You are very welcome!
CDL-1	Coalition for a Secure Driver's License	Brian Zimmer				2	A new section should be added to Section 2 – to require gradual introduction of additional embedded security features in the PIV credential physical document. Currently there is only a requirement for a single security feature. At a minimum, a federal identity card (flash pass) that is not electronically verified except by a commodity level chip is not a reliable identity document, as it may be easily counterfeited by a standard card printer available from many sources. It is typical for a state issued driver's license to have as many as 12 visually confirmable security features on the front and the back of each card. In addition, as few as 1 and as many as 22 hidden security features are placed on cards which can be seen only be optical devices and/or ultra-violet lighting devices. Micro-print is a common security feature that greatly increases the difficulty of counterfeiting. While this will increase the cost of the printers, it will also reduce the likelihood that criminals will counterfeit PIV cards to facilitate common theft, or that espionage will be facilitated through unlawful access to government buildings.		Declined. Since the VIS authentication has been downgraded to "Little or No Confidence", the increased cost of additional printed security features would not be justified.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
CDL-2	Coalition for a Secure Driver's License	Brian Zimmer					Additional security should be added to the card to include (a) the use of composite card materials that disintegrate should image or name alteration be attempted; (2) micro-chips should include an authentication serial number to reduce the counterfeiting risk from "cloning" a PIV card micro-chip so it passes electronic device recognition; (3) an encrypted bar code should be added to the back of the card which includes a unique inventory number for the card that also includes the serial number of the printer on which the card was produced. ICE and other federal agencies regularly apprehend individuals engaged in large scale identity document counterfeiting who rely on "used" commercial card printers, often purchased as government surplus on E-Bay. As long as HPSD-12 PIV cards can be produced on inexpensive commodity card printers, the risk of counterfeiting them increases. It's important to recognize that federal government credentials have been counterfeited including those issued to military personnel and dependents, and also fraudulently produced by "insiders," NOT for the purpose of entering government property but for the purpose of identity fraud and/or criminal purposes. That is, counterfeit identity rings often reproduce government identity credentials as part of a set of fraudulent identity documents expressly to obtain driver's licenses under assumed names, and thus conceal the actual identity of the driver's license applicants.		Declined. Since the VIS authentication has been downgraded to "Little or No Confidence", the increased cost of the proposed security features would not be justified.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
CDL-3	Coalition for a Secure Driver's License	Brian Zimmer				4.1.4.1	Section 4.1.4.1. has been modified to allow names as long as 70 characters inclusive. This modification is welcome, but is inadequate to contain typical names from certain ethnic backgrounds. Further, the name blocks should be expanded to include as many as seven primary name fields. For example, former Guantanamo terrorist suspect Sa'id Ali Jabir Al Khathim Al Shihri (died February 12, 2011[1]), had he been issued an HPSD-12 PIV card, would have not have been able to accurately place his name on the card. Instead, the issuing agency, for example the Department of Defense, would have to compress the name into the three name fields now provided. As you can see, Mr. Shihri requires seven name blocks to accurately capture his entire name. Since it is not uncommon for names from natives of the middle east or from Spain to have as many as seven distinct names, and there is growing immigration from these regions, HPSD-12 governance should be able to incorporate such names in its conventions. To do otherwise is culturally insensitive, as well as contributing to inaccurate and incomplete biographical name distinctions. To incorporate complete names of other regions, especially Southern Asia, the entire name structure should be increased to include 124 characters, both in print and in electronic formatting of the data records system.		Declined. Primary and secondary identifiers can have several words, see examples in Table 4-1.
Cert-1	Certipath PMA	Judith Spencer	E	vi	164		"The Office of Management and Budget (OMB) provides an implementation oversight of this standard." - It leaves the impression that there is other oversight and OMB is just one option.	Recommend removing 'an' from this sentence.	Accept.
Cert-2	Certipath PMA	SPH	E	vi	191		"…technology, the NIST…"	"…technology, NIST…"	Accept.
Cert-3	Certipath PMA	SPH	T	2	243	1.2	"This standard defines authentication mechanisms offering varying degrees of security." is not clear with regard to both logical and physical access gaining equal weighting in this standard.	Proposed text: "This standard defines authentication mechanisms offering varying degrees of security for both logical and physical access applications."	Accept.
Cert-4	Certipath PMA	SPH	E	2	274	1.3.3	This section defines OCC: "...an optional On-Card Biometric comparison (OCC)…" and it is not used consistently throughout the document. And OCC is not a complete acronym.	Use the acronym consistently throughout the document. Recommend changing the acronym to "OCBC" to be consistent with the definition. Alternatively, use the more industry accepted match-on-card (MOC) for this acronym.	Resolved by IBIA-1.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-5	Certipath PMA	SPH	T	3	287	1.3.5	There is no information on adoption/migration between versions of FIPS 201. There needs to be some guidance on distinguishing which version of FIPS 201 was used to issue a given card.	There needs to be a new special publication that specifies adoption practices for the incremental updates of FIPS 201. FIPS 201-2 should reference this document. Specifically, this new SP should cover sunrise and sunset processes, especially in relation to Sections 1.3.3 and Section 1.3.4.	Declined. The change of PIV Card / middleware versions will be managed in SP 800-73-X. Timeline changes will be managed by OMB.
Cert-6	Certipath PMA	SPH	T	3	288	1.3.5	There must be a specific way to tell versions. This dictates how the physical infrastructure will migrate. Current language is "New version numbers may be assigned in [SP 800-73] depending on the nature of the change."	Proposed text: "New version numbers will, at a minimum, be assigned in [SP 800-73] specifically delineating non-backward compatible and deprecated or removed changes. In addition, [SP800-73] must provide a discovery mechanism that addresses changes defined in sections 1.3.1, 1.3.2, 1.3.3, and 1.3.4." This clarifies that 800-73 provides the technical version management and the means to detect changes that drive the physical infrastructure.	Resolved by replacing the sentence "New version numbers may be assigned in [SP 800-73]..." with "New version numbers will be assigned in [SP 800-73], if needed based on the nature of the change. " Noted. Noted. SP 800-73 already defines a discovery mechanism (object) that will be used when appropriate.
Cert-7	Certipath PMA	SPH	T	4	320-322	1.4	PIV Front-End Subsystem actually defines the credential, not a front-end system. Current text: "Section 4, PIV Front-End Subsystem, provides the requirements for the components of the PIV front-end subsystem. Specifically, this section defines requirements for the PIV Card, logical data elements, biometrics, cryptography, and card readers."	Proposed text: "Section 4, PIV Card Requirements, provides the requirements for the components of the PIV card. Specifically, this section defines requirements for the topology of the card, the electronic data model defining specific data elements including biometrics, cryptography. This section also introduces the concept of alternative form factors for future consideration in FIPS 201."	Declined. Section 4 represents requirements for Front-End Subsystem components as described in Figure 3-1.
Cert-8	Certipath PMA	SPH	T	5	358-359	2.1	Current text does not address suitability independently from identity, causing confusion.	Proposed text: "Credentials are issued to individuals whose 1) true identity has been verified, 2) whose suitability has been confirmed, and 3) after a proper authority has authorized issuance of the credential;"	Declined. As noted in the Springer Memo, suitability determination is not required for all PIV Card applicants.
Cert-9	Certipath PMA	Judith Spencer	E	5	360-361	2.1	The completed criminal history check has to be adjudicated favorably before the credential can be issued.	Recommend adding "and favorably adjudicated" to this statement	Declined. Current language is consistent with the Springer Memorandum and M-05-24.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-10	Certipath PMA	SPH	G	6-7	391-437	2.3	This text is very much improved over I-9, but primary and secondary identity documents change over time. FIPS 201 will not have an accurate list that lasts the full five year period.	Move identity proofing document requirements into a special publication.	The US Citizenship and Immigration Service's I-9 identity source document revision history indicates that the list of identity source document remain surprisingly stable, and that changes have tended to be related to verification of employment authorization rather than verification of identity. In order to help ensure the stability of the list of acceptable documents, the following three items will be deleted from the list of acceptable primary identify source documents: • Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa • In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form • Passport from the Federal States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the US and the FSM or RMI and a new item will be added that says: • A foreign passport
Cert-11	Certipath PMA	SPH	T	6-7	391-437	2.3	No guidance is given to establish basic groundrules for comparison of (corroboration) and accuracy between source identity documents.	Ensure the new special publication identified in (comment 13) addresses guidance for comparison/corroboration between identity documents vs. the claimed identity.	Resolved by inserting the sentence in Section 2.3 (now Section 2.7), 4th bullet: "The source documents shall be bound to that applicant."
Cert-12	Certipath PMA	SPH	T	6	394-410	2.3	This list does not include PIV or PIV-I cards.	Add PIV and PIV-I cards. If not for primary, at least for secondary. They are fully electronically verifiable and this is a significant advantage in the identity proofing process. If necessary, require Federal Common and FBCA CPs to be changed to reflect this ID proofing list, enabling this use.	Resolved by replacing the Common Access Card with the PIV Card on the list. Decline adding PIV-I to the list since PIV-I is not guaranteed to be a Federal or State government issued ID.
Cert-13	Certipath PMA	SPH	E	6	393	2.3	"...cancelled, shall be one…"	"...cancelled, and shall be one…"	Accept.
Cert-14	Certipath PMA	SPH	E	6	401	2.3	"...containing an endorsement has not yet expired…"	"...containing an endorsement that has not yet expired…"	Resolved by new text.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-15	Certipath PMA	Judith Spencer	T	7	441	2.3	Recommend including a description of the capture of facial image and biometric as part of the 'chain-of-trust' record. Section 2.3 seems to ignore the collection of these artifacts and concentrate on the id proofing aspects, even though the title of the section includes "registration". Capture of these items as part of the registration process is important in creating the 'chain of trust record, and the reference to Section 4.4.1 does not allow for good flow for the reader, nor does that section provide the information necessary to ensure the reader realizes what the chain-of-trust record is comprised of.	Add a list of the information/artifacts that are included in the 'chain-of-trust' record. Explicitly state that fingerprints are captured during registration and that a facial image is captured and placed in the chain of trust record. See attached suggested language for section 2.3.	Resolved by creating new sections on biometric data collection, biometric data use, and chain-of-trust that are inserted before the "PIV Identity Proofing and Registration Requirements" section. In the Revised Draft FIPS 201-2, maintenance of a chain-of-trust is optional. However, a list of the information/artifacts that are recommended to be included in a chain-of-trust record is provided. The need to protect personally identifiable information stored in the chain-of-trust is also addressed. Decline to require signing chain-of-trust.
Cert-16	Certipath PMA	Judith Spencer	E	8	461-462	2.4	Statement appears incomplete	Recommend adding "record" to "chain-of-trust" in this statement.	Accept.
Cert-17	Certipath PMA	Judith Spencer	E	8	463-469	2.4	It seems that these two items are accomplishing the same thing. One is a general statement, the other describes a specific process.	Recommend combining these two bullets into a single requirement	Accept.
Cert-18	Certipath PMA	Judith Spencer	T	8	473-477	2.4	This paragraph is problemmatic. The first two sentences are fine, but the 3rd and 4th sentences could result in 'almost PIV' cards being reused. It may only affect situations where PIV cards are used as flash passes, but there is no way to know that it is an 'almost PIV' when presented in this fashion. There is no interdiction on electronically personalizing the card either, which could cause more confusion. In the statement "PIV Card issuer is responsible for the card stock, its management, and its integrity. This standard does not place any requirements on these cards," what does it mean? What cards? - scratched or illegible? Or all cards? Card stock needs to be protected, especially "almost PIVs".	Recommend revising this paragraph to clarify meaning, and recommend that the standard specifically state that damaged, erroneous or faded cards should be destroyed.	Resolved by replacing the paragraph with the following: PIV Cards that contain topographical defects (e.g., scratches, poor color, fading, etc) or that are not properly printed shall be destroyed. The PIV Card issuer is responsible for the card stock, its management, and its integrity.
Cert-19	Certipath PMA	SPH	T	9	486-489	2.4.1	The reference to the employee name change section is not really appropriate. That process establishes a legal name change with documentary evidence, then proceeds to re-issuance which requires the issuer to recover the previous card and destroy it. As such, an individual requiring a pseudonymous card can not retain their current PIV card.	Fully specify the requirements for ID Proofing and Issuance of a new PIV card under a pseudonym here. Specifically describe use of existing PIV as authentication for new pseudonymous PIV card. This may reference the re-issuance section, but this section must be clear that the original PIV card does not need to be recovered and destroyed.	Resolved by removing "for employee name changes" from the sentence "The issuance of a PIV Card using a pseudonym shall follow the procedures in PIV Card Issuance Requirements except that the employee must provide evidence satisfactory to the card issuer that the pseudonym is authorized by the employee's agency."
Cert-20	Certipath PMA	Judith Spencer	E	9	491-494	2.4.2	Is this paragraph suggesting that the identity proofing does not need to be repeated. If so, this is not clear.	Recommend revising this paragraph to state that the identity proofing/NACI does not need to be repeated and the original chain-of-trust record can be used to verify identity.	Resolved by new Grace Period text.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-21	Certipath PMA	SPH	T	9	503	2.5	"...Backend Attribute Exchange..." refers to a specific activity underway in FICAM. Recommend the language be more broad in FIPS 201 to allow for advances in technology.	"...Federation Services (including Backend Attribute Exchange)..."	Resolved by removing the sentence: "Background Investigation status information shall be made available to authenticating parties, government-wide, through the Office of Personnel Management (OPM) Central Verification System, Backend Attribute Exchange, or other operational system approved by OMB." See DoD-48.
Cert-22	Certipath PMA	SPH	T	9	506	2.5.1	This section is incorrectly named. Renewal is used very differently in PKI and smart card environments and this incorrectly re-defines renewal. PIV Card Renewal is actually renewing the PKI certificates at the 3 year mark, extending the life of that particular PIV card.	Change section to be: "PIV Card Routine Re-issuance Requirements" as you are not actually renewing the existing PIV Card. -or- pick a different word than "Renewal"	Declined. This is a term that was used in FIPS 201-1.
Cert-23	Certipath PMA	SPH	T	9	507	2.5.1	As discused in Comment 20 above, comments 21-25 recommend the following be revised: "Renewal is the process by which a valid PIV Card is replaced without..."	Recommended revision: "Routine re-issuance is the process by which a PIV card that is reaching its expiration date (at the end of its 6 year lifetime) is replaced without..."	Declined. The term Renewal has been in use since FIPS 201. Using "Routing re-issuance" would confuse readers, especially with the re-issuance term.
Cert-24	Certipath PMA	SPH	T	9	508-510	2.5.1	"The original PIV Card must be surrendered when requesting a renewal. The PIV Card is renewed only after a proper authority has authorized renewal of the credential."	Proposed text: "The original PIV Card must be surrendered during routine re-issuance. A proper authority must authorize routine re-issuance."	Resolved by Cert-23.
Cert-25	Certipath PMA	SPH	T	9	511	2.5.1	"...current before renewing..."	"...current before routine re-issuance of..."	Declined. Resolved by Cert-23.
Cert-26	Certipath PMA	SPH	T	9	517	2.5.1	"...apply for a renewal starting..."	"...apply for routine re-issuance starting..."	Declined. Resolved by Cert-23.
Cert-27	Certipath PMA	SPH	T	9	519	2.5.1	"...renewal process..."	"...routine re-issuance process..."	Declined. Resolved by Cert-23.
Cert-28	Certipath PMA	SPH	T	9	521	2.5.1	This is an open ended requirement with significant system level and privacy concerns. What is the PIV management infrastructure? It is undefined. "...and distribute the changed data within the PIV management infrastructure."	delete "and distribute the changed data within the PIV management infrastructure" from the sentence.	Accept. Delete the extra language at lines 521 and 500.
Cert-29	Certipath PMA	Judith Spencer	E	10	524	2.5.1	This statement begins "The same biometric. . ." Recommend revision to be more specific - same as what?	Recommend revision as follows: "The stored biometric data. . ."	Resolved by replacing: "The same biometric" with "Previously collected biometric"
Cert-30	Certipath PMA	SPH	T	10	525	2.5.1	Although the first sentence sets the minimum requirement, it is not operationally a good idea.	Add proposed sentence after the first sentence: "Issuers may elect to refresh the biometric data after reconnecting the applicant to their chain-of-trust record to improve operational effectiveness."	Resolved by adding the following sentence: As biometric authentication accuracy degrades with the time elapsed since initial collection, issuers may elect to refresh the biometric data after reconnecting the applicant to their chain-of-trust.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-31	Certipath PMA	Judith Spencer	G	10	533-535	2.5.2	There is no mention in this section of the involvement of an 'authorizing official'. Should there be? It seems that if a credential has been compromised, lost, stolen, there should be involvement from the management chain, rather than a purely administrative act of reissuance. Reissuance should carry with it an authorization to reissue the card - closer to original issuance than routine card expiring.	Recommend revising Section 2.5.2 to require management intervention: "A cardholder shall apply for reissuance of a new PIV Card if the old PIV Card has been compromised, lost, stolen, or damaged. The cardholder can also apply for reissuance of a valid PIV Card in the event of an employee status or attribute change or if one or more logical credentials have been compromised. Credentials are reissued only after a proper authority has authorized reissuance of the credential.	Declined. The credential is already authorized. FIPS 201 does require authorization if the card is re-issued with extended expiration date.
Cert-32	Certipath PMA	SPH	E	10	538	2.5.2	"(see Section 4.4.1)"	See comment 15. Amend to reference section 2.3 which establishes the chain-of-trust as a function of initial enrollment and issuance.	Resolved by AMAG-6.
Cert-33	Certipath PMA	Judith Spencer	E	10	544	2.5.2	Recommend being more precise with this language to avoid any confusion since a new card is being issued, and it is the lost, stolen, damaged card that the bullets relate to.	When reissuing a PIV Card, normal operational procedures must be in place to ensure the following in respect to the lost, stolen, damaged or compromised PIV Card:	Resolved by replacing: "When reissuing a PIV Card, normal operational procedures must be in place to ensure the following:" with: "When reissuing a PIV Card, normal revocation procedures must be in place for the compromised, lost, stolen, or damaged card to ensure the following:"
Cert-34	Certipath PMA	SPH	T	10	545-546	2.5.2	"The PIV Card itself is revoked. Any local databases that contain FASC-N values must be updated to reflect the change in status." Updating local databases is an open ended requirement. There is no way for the issuer to know where all the relying party databases that contain these values are. Revocation of a PIV Card is explicitly tied to the PIV Auth Cert. There is no other interoperable means of revoking a PIV Card.	Remove this bullet. The requirement is correctly stated in lines 547-556. All relying party systems are obligated to check the CRL/OCSP responders.	Declined. This text does not impose requirement on all relying system databases.
Cert-35	Certipath PMA	Judith Spencer	E	10	557	2.5.2	See Comment 33 above, recommend the reference to the PIV card is explicit.	The damaged or compromised PIV Card shall be collected and destroyed if possible.	Declined. All PIV Cards should be collected and destroyed whenever they are replaced with new cards.
Cert-36	Certipath PMA	SPH	T	10	557-558	2.5.2	"If the card cannot be collected, normal operational procedures shall be completed within 18 hours of notification." Normal operational procedures are not clear. Implies revocation.	Proposed text: "If the card cannot be collected, normal revocation procedures shall be completed within 18 hours of notification."	Accept to change “operational” to “revocation” on lines 544 and 558.
Cert-37	Certipath PMA	SPH	T	10-11	564-566	2.5.2	Although this sentence sets the minimum requirement, it is not operationally a good idea.	Add proposed sentence after this sentence: "Issuers may elect to refresh the biometric data after reconnecting the applicant to their chain-of-trust record to improve operational effectiveness."	Resolved by NIST-89. In addition add the following text in Section 4.4.1 (now Section 2.6) after line 1349: "In order to mitigate ageing effects and thereby maintain operational readiness of a cardholder's PIV card, agencies may require biometric enrollment more frequently than 12 years."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-38	Certipath PMA	SPH	T	11	579	2.5.3	Re-Key is a special case of post issuance update	Add new last sentence: "Re-Key shall follow the requirements in section 2.5.4."	Resolved by removing Section 2.5.3, since re-keying is already covered in Section 2.5.4 (now Section 2.9.3).
Cert-39	Certipath PMA	SPH	T	12	604-607	2.5.5	Need to separate cardholder changing their PIN when they know the old PIN, from issuer doing a reset on PIN block or PIN forgotten.	Proposed text: "The PIN on a PIV Card may need to be reset if the cardholder wants to change their PIN, if the cardholder has forgotten the PIN, or if PIN-based cardholder authentication has been disabled from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency (PIN blocked). If the cardholder knows the current PIN and the card and the card is not PIN blocked, the cardholder may reset their PIN upon presentation of the current PIN to the card. PIN resets may be performed by the card issuer. ..."	Resolved by removing PIN change from the text since PIN change is not the same as PIN Reset. Also, added the footnote: Cardholders may change their PINs anytime by providing the current PIN and the new PIN values.
Cert-40	Certipath PMA	SPH	T	12	608-620	2.5.5	Issuer reset of verification data includes both PIN and biometric on card comparison reference data. There are not separate procedures for either of these as far as the issuer is concerned. Start a new paragraph and replace the text beginning with "PIN resets may be performed..." The proposed text for 1:1 match against the chain-of-trust is equivalent to the requirements in PIV-I for verification data (PIN) reset, maintaining the overall security of both PIV and PIV-I.	Proposed text: "The card issuer may reset verification data (including the PIN or on card biometric comparison data). Before resetting the PIV Card verification data, the card issuer shall reconnect the cardholder to the chain-of-trust record by performing a 1:1 match of the cardholder (see section 2.3). Upon successful match, the issuer may reset PIV Card verification data.[footnote 3] Departments and agencies may adopt more stringent procedures for verification data reset (including requiring in-person appearance or disallowing verification data reset, and requiring the termination of PIV Cards that have been locked); such procedures shall be formally documented by each department and agency."	Declined – The final three paragraphs in Section 2.9.4 (formerly Section 2.5.5) address the requirement for resetting biometric data. These requirements are different from PIN reset and should not be combined.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-41	Certipath PMA	SPH	T	12	621	before 2.5.6	There is no definition on what constitutes a revoked or expired PIV card. Per the workshop, the proposed language is offered to correct the hassles of "too many expiration dates".	Add the following section: 2.5.x PIV Card Revocation/Expiration Status A PIV Card is revoked if any of the following is true: - The PIV Authentication Certificate is revoked or PDVAL fails for the trust chain - The Card Authentication Certificate is revoked or PDVAL fails for the trust chain A PIV Card is expired if any of the following are true: - The PIV Authentication Certificate is expired - The Card Authentication Certificate is expired All relying party applications shall have normal operating procedures to verify revocation and expiration status of PIV Cards according to policy. No relying party application shall rely upon a revoked or expired PIV Card. The expiration dates in the authentication certificates will always expire on or before the CHUID expiration date. Therefore relying party applications should always check the authentication certificates.	Declined as follows: An authentication certificate (and its associated key pair) may be revoked without revoking the PIV Card and may then be replaced. Also, PDVAL may fail as a result of intermittent problems, such as a repository being temporarily unavailable, and this would not be an indication that the card is revoked. The card expiration date is the date that is printed on the card and also appears on the CHUID. The authentication certificates, on the other hand, may expire before the card expires. Resolved by Cert-104. Resolved by Cert-104.
Cert-42	Certipath PMA	Judith Spencer	E	12	624-625	2.5.6	PIV Cards are also terminated for the reasons indicated in Section 2.5.2, this should be referenced here.	Recommend modifying the sentence that begins on line 624 as follows: "In addition to the scenarios identified in Section 2.5.2, the PIV Card shall be terminated under the following circumstances:"	Resolved by deleting the the following sentence from the beginning of Section 2.5.6 (now Section 2.9.5): The termination process is used to permanently destroy or invalidate the use of a card, including the data and the keys on it, such that it cannot be used again.
Cert-43	Certipath PMA	SPH	T	13	643	2.5.6	IIF is not defined. Isn't this Personally Identifiable Information (PII)?	Replace with: "The PII collected from the cardholder…"	Accept use of PII. Resolved by replacing all instances of IIF by PII. We will define PII with a reference to OMB M-07-16. Also, delete IIF from the glossary.
Cert-44	Certipath PMA	SPH	E	13	645	2.5	The reference to Appendix C is the last sentence of section 2.5. It belongs in Section 2.5 (line 496). It flows better and does not hide the reference in section 2.5.6 which is only about termination. Appendix C covers a lot more than termination.	Move the sentence at 645 to line 496 adding it as a second sentence: "A summary of PIV Card Issuance and PIV Card Maintenance requirements is provided in Appendix C."	Resolved by deleting Appendix C and by deleting the referenced sentence.
Cert-45	Certipath PMA	Judith Spencer	E	13	660	2.6	This sentence has been cut too severely, recommend you restore the 'departments and agencies shall' otherwise there is no context for the following bullets.	To ensure the privacy throughout PIV life cycle departments and agencies shall:	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-46	Certipath PMA	Judith Spencer	E	13	675-676	2.6	Syntax! This bullet should be reworded to follow established syntax for the bullet list. Also, recommend that it refer to use of the data not use of the PIV card, since usage could change over time as new applications are developed. Also, recommend not giving agencies the incentive to limit use of the PIV card.	Recommend modifying this bullet as follows: Provide PIV applicants ~~shall be provided~~ full disclosure of the intended uses of the information associated with the PIV credential and the related privacy implications.	Resolved by combining bullets 3 and 4, fixing the parenthesis in bullet 3, and using the proposed language for the last sentence.
Cert-47	Certipath PMA	SPH	T	15-19	698-826	3	This section is very clearly out of sync with the FICAM Segment Architecture and the FICAM Roadmap. Specifically, Figure 3-1 and the definitions that support it are no longer notionally correct.	This must be updated to harmonize with the FICAM Roadmap and Implementation Guidance v1.0, dated November 10, 2009, Section 2. This is the best federal document that defines ICAM architecture. This will clarify the separation of Identity Management and Credential Management from Access Management and reduce confusion in subsequent sections that merge these concepts using the current definitions in Section 3. See notional text for Section 3	Declined. FIPS 201 is not in conflict with FICAM. FIPS 201 does not have the charter for enterprise architecture; therefore, the simple notional diagram to address PIV requirements already serves the needed purpose. Moreover, changing terms would cause more harm since these terms have been in effect for over 7 years. This is a major change to the document that is unnecessary.
Cert-48	Certipath PMA	Judith Spencer	E	15	698	3	Recommend removal of the opening sentence (A notional PIV system architecture. . .). At the end of this paragraph, it is stated that "The following sections briefly discuss the functional components of the PIV system and the life cycle activities of the PIV Card." This is a more accurate description of the chapter and suffices.	Remove opening sentence.	Accept.
Cert-49	Certipath PMA	Judith Spencer	T	16	754-755	3.1.1	From the description here, card writers would not be in the 'front end system' but in the card issuance and management system. Card writers in this context would be used for remote update of the card (rekey etc) and this should be mentioned here.	Recommend revising this sentence as follows: "Card writers that are very similar to the card readers personalize and initialize the information stored on PIV Cards and may also be used to perform remote PIV card updates (see Section 2.5.4)."	Resolved by replacing the referenced sentence with the following two sentences: Card writers, which are very similar to the card readers, personalize and initialize the information stored on PIV Cards. Card writers may also be used to perform remote PIV Card updates (see Section 2.9.3).

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-50	Certipath PMA	Judith Spencer	E	17	757-766	3.1.1	These two paragraphs seem to be in reverse order. Recommend discussing PIN first and then biometric. The final sentence of the PIN paragraph (This provides for a higher level of authentication assurance.) could then be transferred to the biometric paragraph, which is a more appropriate location for it.	Reverse order of the paragraph on card plus pin and card plus bio, and move last sentence of pin paragraph to bio paragraph.	Accept. Replace: PIN input devices can also be used along with card readers when a higher level of authentication assurance is required. The cardholder presenting the PIV Card must type in his or her PIN into the PIN input device. For physical access, the PIN is typically entered using a PIN pad device; a keyboard is generally used for logical access. The input of a PIN introduces provides a the use of an additional factor of authentication ("something you know") authentication factor that activates the PIV card and enables to control access to other credentials information resident on the card that provide additional factors of authentication. A cryptographic key and certificate, for example, provides an additional authentication factor of ("something you have") (e.g. the card) through PKI-based authentication. This provides for a higher level of authentication assurance. Biometric readers may be located at secure locations where a cardholder may want to gain access. These readers depend upon the use of biometric data of the cardholder, stored in the memory of the card, and its comparison with a real-time biometric sample. The use of biometrics provides an additional factor of authentication ("something you are") in addition in addition to entering the PIN ("something you know") and to providing the card ("something you have") for cryptographic key-based authentication. This provides for a higher level of authentication assurance. with: PIN input devices can be used along with card readers when a higher level of authentication assurance is required. The cardholder presenting the PIV Card must type in his or her PIN into the PIN input device. For physical access, the PIN is typically entered using a PIN pad device; a keyboard is generally used for logical access. The input of a PIN provides a "something you know" authentication factor that activates the PIV card and enables access to other credentials resident on the card that provide additional factors of authentication. A cryptographic key and certificate, for example, provides an additional authentication factor of "something you have" (e.g. the card) through PKI-based authentication. Biometric readers may be located at secure locations where a cardholder may want to gain access. These readers depend upon the use of biometric data of the cardholder, stored in the memory of the card, and its comparison with a real-time biometric sample. The use of biometrics provides an additional factor of authentication ("something you are") in addition in addition to entering the PIN ("something you know") and providing the card ("something you have") for cryptographic key-based authentication ("something you have"). This provides for a higher level of authentication assurance.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-51	Certipath PMA	Judith Spencer	T	17	796-797	3.1.3	Information may not be cardholder-provided. In some cases, there may be recourse to a backend data base for additional information. Also I&A must interact with the authz component at some point - not mentioned.	Recommend revising this sentence as follows: "Once authenticated, the I&A component passes information to the authorization component which in turn interacts with the authorization data component to match the cardholder~~-provided~~ information to the information on record."	Accept.
Cert-52	Certipath PMA	Judith Spencer	T	18	798-799	3.1.3	The previous paragraph indicates the authorization component is part of the access control component. Also, no mention of back end attribute exchange - could be mentioned here. Finally, Federal PKI requires the availability of certificate status services for PIV, so the qualifiers are not needed.	Recommend revising this sentence as follows: "The access control components typically interface with the card reader, ~~the authorization component,~~ the PIN input device, the biometric reader, supplementary databases, and ~~any~~ certificate status service ~~(if available)~~."	Resolved by replacing: "The access control components typically interface with the card reader, the authorization component, the PIN input device, the biometric reader, supplementary databases, and any certificate status service (if available)." with: "Access control components typically interface with the card reader, the PIN input device, the biometric reader, supplementary databases, and any certificate status service.
Cert-53	Certipath PMA	Judith Spencer	E	18	811-813	3.2	Recommend the second bullet also include capture of biometrics information, capture of facial image, and creation of chain-of-trust record.	Modify the second bullet as follows: **"Identity Proofing and Registration.** The goal of this activity is to: verify the claimed identity of the applicant and that the entire set of identity source documents presented at the time of registration is valid; capture biometrics and facial images; and create the chain-of-trust record."	Accept as The goal of this activity is to verify the claimed identity of the applicant, verify that the entire set of identity source documents presented at the time of registration is valid, capture biometrics, and optionally create the chain-of-trust record."
Cert-54	Certipath PMA	SPH	E	20	827	4	This section does not define a "Front-End Subsystem". It actually defines the PIV Card.	Rename the section. Proposed title: "PIV Card Requirements"	Declined. The Front-End Subsystem, as depicted in Figure 3-1 includes more than PIV Cards.
Cert-55	Certipath PMA	SPH	T	20	828	4	Current text: "This section identifies the requirements for the components of the PIV front-end subsystem."	Proposed text: "This section identifies the requirements for the PIV Card."	Declined. This section also includes requirements for card reader, PIN device, and biometric reader.
Cert-56	Certipath PMA	SPH	T	20	832	4	Current text: "Section 4.5 discusses card readers." This is the only section that is not directly related to the definition of the PIV Card. No new requirements are outlined (beyond conformance to ISO stds and SP800 series). It is very incomplete (wrt PACS in particular).	If Section 4.5 must be retained, proposed text: "Section 4.5 discusses card readers, providing minimum mandatory requirements for security and interoperability with the PIV Card."	Resolved by revising the sentence to "Section 4.4 provides requirements for PIV Card readers."
Cert-57	Certipath PMA	SPH	T	20-36	833 thru 1122	4.1.1 thru 4.1.5	Card topology specifications are split between FIPS 201-2 and SP 800-104	Move all physical card and topology definitions (specifically sections 4.1.1 thru 4.1.5) into SP800-104 and make this a normative reference from FIPS 201-2.	Resolved by moving information from SP 800-104 to FIPS 201-2 and making Zone 15F and 18F mandatory. Also, withdraw SP 800-104.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-58	Certipath PMA	SPH	T	20	845	4.1	In accord with comment (57), make SP800-104 reference normative.	Add the following proposed text after "...[ISO14443].": "The specifications for the physical card and topology of a PIV Card are defined in [SP800-104]. These specifications include: - Printed Material - Tamper Proofing and Resistance - Physical Characteristics and Durability - Visual Card Topography - Color Representation"	Resolved by Cert-57.
Cert-59	Certipath PMA	SPH	T	21	943-951	4.1.4.1	Zone 2F attempts to define an authoritative name to be printed on the credential. Zone 2F and the corresponding entries in the printed information buffer are for human verification. These should not be confused with the authoritative names in the PKI credentials. Recommend the use of nicknames be permitted on line 2 of Zone 2F at the PIV card owner's discretion. ie. Polk, W. Tim, instead of Polk, William T.	This needs to be amended to define a Primary Printed Identifier and a Secondary Printed Identifier used for human visual verification. These identifiers shall be stored in the Printed Information Buffer defined by [SP800-73]. The Primary identifier is the last name (including generational identifier and punctuation). The Secondary identifier can be a common given name used on a daily basis (including nicknames and punctuation).	Declined. As per OMB, the primary and secondary identifier should only be the name verified through source document. Nicknames are not allowed / accepted. The visual and stored names should also be the same.
Cert-60	Certipath PMA	Judith Spencer	T	25	1010	4.1.4.3	Recommend removing this item. PIV card issuance practice is to place the FERO indicator at the bottom of the card. Placing it in this location is redundant and will obscure the contractor/foreign national indicator. This practice should be deprecated	Remove this bullet.	Resolved by removing "Red" from the list and adding "White" color to the list, remove bar and description of "FERO" from Figure 4-4, and revise the first sentence on line 998 to: The footer is the location for the Federal Emergency Response Official identification label.
Cert-61	Certipath PMA	Judith Spencer	T	25	1005-1014	4.1.4.3	Order of precedence? If a contractor is a foreign national which color is used? Is this left to the agency? Interoperability is affected if the color coding precedence is not universally agreed upon across the Federal enterprise.	Recommend this section include a statement on color code precedence.	Resolved by adding the following SP 800-104 precedence text in Section 4.1.4.1: "Foreign National color-coding has precedence over Government Employee and Contractor color-coding. " (Note: resolution of Cert-60 removed “Red” and added “White”)
Cert-62	Certipath PMA	Judith Spencer	E	36	1123-1176	4.1.6 - 4.1.7 4.2 - 4.4	I don't understand why this discussion of logical features is included in a section titled "Physical Characteristics". It is clearly not. The current 4.2 through 4.4 could then be included as subsections of the new Section 4.2 as they are clearly Logical characteristics. This has bugged me since FIPS 201 was first released, and this would be an opportunity to fix it.	Recommend creating a new Section 4.2 titled "Logical PIV Card Characteristics" and renumber Sections 4.1.6 and 4.1.7 as Sections 4.2.1 and 4.2.2 respectively. Then current Sections 4.2 through 4.4 would beocme 4.2.3 thorugh 4.2.5 respectively.	Resolved by AMAG-6.
Cert-63	Certipath PMA	SPH	T	36	1124	4.1.6	In concert with (62), "This section defines logical identity credentials and the requirements for use of these credentials." is not accurate.	Proposed text: "This section defines the PIV Card Application and Data Model. This provides the definition of PIV Card identity credentials and the requirements for the application that manages these credentials on the PIV Card."	Resolved by AMAG-6.
Cert-64	Certipath PMA	SPH	T	36	1125	4.1.6.1	In concert with (62), this section defines the PIV Card Data Model.	Rename section and make it level 3 in concert with (48). Proposed: "4.2.1 PIV Card Data Model"	Resolved by AMAG-6.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-65	Certipath PMA	SPH	T	36	1126-1128	4.1.6.1	In concert with (62), current text must be updated to reflect clarity in data model vs. logical credentials within the data model.	Proposed text: "...the PIV Card Data Model shall contain logical credentials composed of multiple data elements as specified in [SP800-73]. These data elements are for the purpose of verifying the cardholder's identity at graduated assurance levels. The mandatory data elements for a PIV Card are:"	Resolved by AMAG-6.
Cert-66	Certipath PMA	SPH	T	37	1140	4.1.6.1	Facial image is optional. Most issuers are coding this on their cards today. Given card technology improvements, there is now sufficient space on the cards. Further, handheld verification devices need the photo for verification by guards. PIV-I makes the facial image mandatory. For interoperability, PIV should do the same.	Make the facial image mandatory.	Accept.
Cert-67	Certipath PMA	SPH	T	37	1150	4.1.6.1	Reference to PIN only in "The PIN falls into the first category..." This doesn't take into account the addition of the on-card biometric comparison which was added in 1.3.3	Proposed text: "The PIN and on card biometric comparison data fall into the first category..."	Resolved by disposition of IGL-16.
Cert-68	Certipath PMA	SPH	T	37-38	1152, 1158, 1169	4.1.7, 4.1.7.2, 4.1.7.2	These sections define application behavior and not the data model. Re-order in concert with (62).	Renumber as follows: 4.1.4 becomes 4.2.2; 4.1.7.1 becomes 4.2.2.2; 4.1.7.2 becomes 4.2.2.2	Resolved by AMAG-6.
Cert-69	Certipath PMA	SPH	T	37	1161	4.1.7.1	"Other card activation..." All modes of activation should be discoverable, including PIN.	Recommend removal of the word "other" as follows: "At a minimum, the PIV Card shall implement PIN-based cardholder activation in support of interoperability across departments and agencies. ~~Other~~ Card activation mechanisms, only as specified in [SP 800-73], may be implemented and shall be discoverable."	Declined. The PIN card activation method is the default method and should therefore activate the card without the need for discovery.
Cert-70	Certipath PMA	SPH	T	38	1177, 1188, 1193	4.2, 4.2.1, 4.2.2	In concert with (62), these sections define the CHUID within the card data model. Renumber as part of section 4.1.	Renumber as follows: 4.2 becomes 4.1.2; 4.2.1 becomes 4.1.2.1; 4.2.2 becomes 4.1.2.2	Resolved by AMAG-6.
Cert-71	Certipath PMA	SPH	T	38	1178-1181	4.2	This should define explicitly what the mandatory and optional data elements are in the CHUID. Recommend that the UUID be made mandatory . The details of formatting should be specified in [SP800-73], not in FIPS 201.	Replace the paragraph with this proposed text: "The PIV Card shall include the CHUID as specified in [SP800-73]. The following fields are mandatory in the CHUID: - FASC-N - GUID - Expiration Date - Issuer Asymmetric Signature"	Resolved by DoD-41.
Cert-72	Certipath PMA	SPH	T	38	1183	4.2	Remove the following: "The PIV FASC-N shall not be modified post-issuance." See comment below for relocation of this requirement.	Remove this language from this section.	Declined.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-73	Certipath PMA	SPH	T	38	1184-1187	4.2	This paragraph is not correct. The CHUID is a static identifier. It is equivalent to a Userid. The CHUID is _not_ equivalent to a password. As it is an identifier, it should _never_ be used as an authenticator requiring the protection described in this paragraph.	Delete 1184 through 1187. There is no need for this paragraph.	Accept.
Cert-74	Certipath PMA	SPH	T	38	1188-1192	4.2.1	Consider deleting this paragraph as not necessary. Replace this with a new section describing the credential identifier usage. See comment 71, recommend making the UUID mandatory for inclusion in the CHUID.	Replace Section 4.2.1 with the following: "The CHUID contains two credential identifiers that are unique to a given PIV card: FASC-N Identifier and a UUID. A subset of the FASC-N, the FASC-N Identifier, shall be unique to the PIV Card and is the concatenation of the Agency Code||System Code||Credential Number fields of the FASC-N. The UUID shall be unique to the PIV Card and is an RFC 4122 compliant Universally Unique Identifier. The UUID is stored in the GUID. The UUID and the FASC-N Identifier shall be used to link signed objects together within the PIV Card, as specified in [SP800-73] and [SP800-76]. The PIV FASC-N shall not be modified post issuance. The UUID shall not be modified post issuance."	Resolved by deleting paragraph and moving relevant text to previous section.
Cert-75	Certipath PMA	SPH	T	38-39	1199-1218	4.2.2	These details belong in SP 800-73 Part 1.	Move to SP 800-73 Part 1.	Accept. Text and associated comments will be addressed in SP 800-73-x.
Cert-76	Certipath PMA	SPH	T	39	1219-1223	4.2.2	This section should identify the issuer asymmetric signature file as a "content signing certificate" and, in light of Advanced Persistent Threats, use of software certificates for content signing should no longer be allowed, therefore remove id-fpki-common-devices as an approved credential type as this is a software based credential.	Delete references to id-fpki-common-devices from this paragraph. Also recommend that Federal PKI be asked to establish a distinct policy OID in COMMON to support content signing credentials.	Resolved by NIST-16 and ICAMSC-96. The Federal PKIPA was asked to establish a distinct policy OID. Also, now refer to certificate needed to verify signature on CHUID and biometric data as "content signing certificate."
Cert-77	Certipath PMA	SPH	T	39	1223	4.2.2	The CMS, PIV Content Signing Key, and Card Management Key do not have specific requirements that they must be protected at the same level as CA systems and keys. When developing the PIV-I guidance, this was specifically required. Recommend FIPS 201 include the same requirement.	Add a sentence to the end of Section 4.2.2 that states: "The Card Management System, PIV Content Signing Key and the Card Management master key must be protected in accord with CA level systems." Work with FPKIPA to update Common and FBCA CPs to reflect this change.	Declined to add text to FIPS 201-2, however FPKIPA could impose such requirements through COMMON.
Cert-78	Certipath PMA	SPH	T	39	1231-1233	4.3	Once a secure channel is established, whether contact or contactless, all operations are allowed through the secure channel.	Allow PIN/Biometric verification, PKI operations, and read of all PIN protected services of a PIV Card through a secure channel (contact or contactless).	Resolved by AI-7.
Cert-79	Certipath PMA	SPH	T	40	1246	4.3	The PIV Auth cert authenticates the cardholder, not just the card. Current text "…and supports card authentication for…"	Proposed text: "…and supports authentication of the card and cardholder for…"	Resolved by DoD-43.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-80	Certipath PMA	SPH	T	40	1250	4.3	This key should be allowed to establish a secure channel, not just card authentication.	Add a new second sentence: "This key may also be used with secure messaging protocols as specified in [SP 800-73]."	Declined. Since the Card Authentication key is under the control of the cardholder, it is not possible to use this key to establish secure session keys. Furthermore, FIPS 186-3 says that "a key pair used for digital signature generation and verification as specified in this Standard shall not be used for any other purpose."
Cert-81	Certipath PMA	SPH	T	40	1260-1261	4.3	Recommend the example be removed. Any keys used for biometric on-card comparison would need to be mandatory in order to ensure interoperability across the federal enterprise.	Add second sentence: "These key(s) may not be interoperable across the federal enterprise."	Declined. This bulleted list identifies the mandatory keys as interoperable across agency use. It is not necessary to point out that optional keys do not provide cross agency interoperability.
Cert-82	Certipath PMA	Judith Spencer	T	40	1267-1281	4.3	The Universal Unique Identifier must be included in addition to FASC-N. Now that PIV-I has been published, and the use of the UUID is discussed in SP 800-73, we should begin shifting to the UUID as a standard alternative and recommending its use in the digital credentials.	Add a sentence to this section to require inclusion of the UUID in addition to the FASC-N in the subjectaltname field.	Accept.
Cert-83	Certipath PMA	SPH	E	41	1281	4.3	"...infrastructure for PIV authentication…"	...infrastructure for the PIV authentication…	Accept.
Cert-84	Certipath PMA	Judith Spencer	T	41	1282-1292	4.3	See comment 82 above. Include UUID as an entry in subjectaltname field.	Add a sentence to this section requiring inclusion of the UUID in addition to the FASC-N in the subjectaltname field.	Accept.
Cert-85	Certipath PMA	SPH	T	41	1293-1298	4.3	If using protocols like Opacity or MR PIV, symmetric keys are established without issuer involvement.	State that there may be more than one symmetric card authentication key and that it may be imported by the issuer or as part of a secure messaging protocol.	Declined. The text in lines 1293-1298 is specific to the symmetric card authentication key (i.e., key reference '9E').
Cert-86	Certipath PMA	SPH	T	41	1296	4.3	"The card authentication key shall be available…"	"Protocols using symmetric card authentication key(s) shall be available…"	Resolved by replacing "The card authentication key shall be available through the contact and the contactless interface of the PIV Card." with: "Cryptographic operations that use the Card Authentication key shall be available through the contact and the contactless interfaces of the PIV Card."
Cert-87	Certipath PMA	SPH	E	42	1316	4.4	This is card application specific.	In concert with comment (48), re-number to 4.2.4.	Resolved by AMAG-6.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-88	Certipath PMA	Judith Spencer	T	42	1328	4.4	There needs to be a positive connection between the fingerprints submitted to FBI and the fingerprints on the card. The statement here does not go far enough if the identity/proofing process is not completed during a single session. Recommend additional language to make this clear. While there is a discussion in the following section (4.4.1), I am concerned this important point could be missed, and should therefore be discussed here as well. Also the language used in the following section is not plain on this point, rather relying on a footnote to get its point across.	Suggested language: All biometric data enumerated above are collected during the identity proofing and registration process. The two fingerprints captured for the PIV card must be collected during the same in person session as the 10-prints or a one-to-one match must be conducted between the two sets of prints to prevent substitution. Iris images, when collected, must be captured during the same session as the 10-print capture. The two prints and/or iris images are subsequently included in the chain of trust record.	Resolved by clarifying that a 1:1 match is required for biometric data collected on different visits.
Cert-89	Certipath PMA	SPH	T	42	1331	4.4	"...the contact interface..." should allow secure messaging access for contactless biometric operations in PACS. This applies equally between on card comparison and off card comparison of the two electronic fingerprints.	Proposed text: "The PIV biometric data, except for on-card biometric comparison data, stored on the card shall be only accessible through the contact interface and after the presentation of a valid PIN. Contact and contactless access of the PIV biometric data is allowed through a secure messaging protocol without presentation of a PIN. After a secure messaging session has been established, cardholder verification using on-card biometric comparison data may be available through the contact and the contactless interface of the PIV Card to support card activation (section 4.1.7.1) and cardholder authentication (section 6.2.5). The PIV Card shall not permit exportation of the on-card biometric comparison data. If implemented, PIV on-card biometric comparison data shall be implemented and used in accordance with [SP 800-73] and [SP 800-76]."	Declined. While Draft FIPS 201-2 permits on-card biometric comparison to be performed over the contactless interface, and will permit the other biometric data to be read over the contactless interface (under certain circumstances), presentation of a PIN will remain a requirement to read the biometric data.
Cert-90	Certipath PMA	SPH	T	42-44	1338-1414	4.4.1	The definition of biometric chain-of-trust is critical to Section 2.3 and should be defined there.	See comment 15. Delete section 4.4.1 as it has moved into section 2.3 as part of ID Proofing and Registration Requirements	Resolved by disposition of AMAG-6.
Cert-91	Certipath PMA	SPH	T	44	1421	4.4.2	"The format for CBEFF_HEADER is specified in [SP 800-76]."	"The format for the biometric data, the CBEFF_HEADER and the CBEFF_SIGNATURE_BLOCK are specified in [SP 800-76]."	Declined.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-92	Certipath PMA	SPH	T	44-45	1422-1453	4.4.2	This defines the details of the signature block.	Move this entirely into [SP800-76].	Accept to move 1429-1453 to 800-76. Also replace 1422-1429: The CBEFF_SIGNATURE_BLOCK contains the digital signature of the biometric data and thus facilitates the verification of integrity of the biometric data. The process of generating a CBEFF_SIGNATURE_BLOCK is described as follows. The CBEFF_SIGNATURE_BLOCK shall be encoded as a CMS external digital signature as defined in [RFC5652]. The digital signature shall be computed over the entire CBEFF structure except the CBEFF_SIGNATURE_BLOCK itself (which means that it includes the CBEFF_HEADER and the biometric records). The algorithm and key size requirements for the digital signature are detailed in [SP 800-78]. with The CBEFF_SIGNATURE_BLOCK contains the digital signature of the biometric data and thus facilitates the verification of integrity of the biometric data. The CBEFF_SIGNATURE_BLOCK shall be encoded as a CMS external digital signature as specified in [SP 800-76]. The algorithm and key size requirements for the digital signature and digest algorithm are detailed in [SP 800-78]. Also move The digital signature shall be computed over the entire CBEFF structure except the CBEFF_SIGNATURE_BLOCK itself (which means that it includes the CBEFF_HEADER and the biometric records). to 800-76-2 Move the requirement to use [RFC5652] to SP 800-76-2.
Cert-93	Certipath PMA	SPH	T	45-46	1454-1458	4.4.2	See comment 76 concerning content signing keys. id-fpki-common-devices software certificates should not be allowed.	Delete references to id-fpki-common-devices which is a software level of assurance.	Resolved by Cert-76.
Cert-94	Certipath PMA	SPH	E	46	1459-1464	4.4.3	Not sure what value this section adds to the document. It is primarily duplicative and referential.	Recommend deleting or repurposing this section.	Accept.
Cert-95	Certipath PMA	SPH	E	46	1465	4.5	This is over and above card data model and card application.	In concert with (62), renumber this section as 4.3	Resolved by AMAG-6.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-96	Certipath PMA	SPH	T	46	1466-1483	4.5	All reader specifications and requirements should be in [SP800-96]. In addition, application of ISO24727 is much broader than just the reader. In particular, the interfaces are more at a system level protecting the application from variations in card profiles. Commerce should look at 24727, GICS and propose profiles for both to minimize change throughout the Federal enterprise. This is out of place in the FIPS 201, which defines the PIV Card, its content, and its issuance requirements.	Replace with: " The minimum requirements for contact and contactless card readers are specified in [SP800-96] and delete subsections 4.5.1 through 4.5.3. Consider conducting a review of SP 800-96 to ensure it is still current and relevant.	Resolved by ICAMSC-126 and ICAMSC-127. Noted. All the SPs will be reviewed in light of the new revision of FIPS 201 specs.
Cert-97	Certipath PMA	SPH	E	47	1495	4.5.4	renumber this section in concert with 102	Renumber to 4.3.1	Resolved by AMAG-6.
Cert-98	Certipath PMA	SPH	T	47	1495-1501	4.5.4	This section applies to any card activation data, not just PIN. It also needs to address biometric as well as PIN in the discussion.	Rename "Card Activation Device Requirements" Revise this section to recommend integrated devices not part of a PC for all card activation (biometric or PIN). Lines 1499-1501 should be more explicit concerning establishing a secure session.	Resolved as follows: Lines 1499-1501 are unchanged since the original FIPS 201 and are not intended to require secure messaging nor secure session. Change title by replacing "4.5.4 PIN Input Device Requirements" with "4.4.4 Card Activation Device Requirements" Modify text to support PIN and On-Card Comparison data as follows: When the PIV Card is used with OCC data or a PIN for physical access, the input device shall be integrated with the PIV Card reader. When the PIV Card is used with OCC data or a PIN for logical access (e.g., to authenticate to a Web site or other server), the input device is not required to be integrated with the PIV Card reader. If the input device is not integrated with the PIV Card reader, the OCC data or the PIN shall be transmitted securely and directly to the PIV Card for card activation. The specifications for fingerprint capture devices for on-card comparison are given in [SP 800-76].
Cert-99	Certipath PMA	Judith Spencer	T	49	1573	5.5.1	LDAP is no longer the best solution and is being replaced with HTTP. Among the issues is the trend that has many firewalls blocking oubound LDAP, which in turn causes validation failures and results in denial of service failures. Recommend this language reflect this reality and start moving us away from LDAP.	This standard requires distribution of CA certificates and CRLs using LDAP and Hypertext Transport Protocol (HTTP) and, optionally, LDAP. Specific requirements are found in the Shared Service Provider Repository Service Requirements [SSP REP].	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-100	Certipath PMA	Judith Spencer	E	51	1606-1607	6.1	Recommend the identity proofing be equated to M-04-04, which has set this standard.	Section 2 of this standard defines requirements for the identity proofing, registration, issuance, and maintenance processes for PIV Cards and establishes a common level of assurance in these processes, which meets E-Authentication Assurance Level 4.	Resolved by adding that PIV ID proofing, registration, issuance, and maintenance processes meet and exceed E-Authentication Assurance Level 4.
Cert-101	Certipath PMA	SPH	T	52-58	1637-1815	6.2	These methods of authentication and their assurance levels are outdated in regards to PACS. The operational sequences are optimized differently than on PCs. Leveraging the PAK or CAK certificate in place of reading the CHUID is often done and just as valid.	Update these authentication scenarios and their assurance levels in accord with the Federated PACS Guidance document from the FICAM AWG.	Resolved by downgrading CHUID and VIS and by adding LITTLE or NO ASSURANCE level to Tables 6-2 and 6-3. Also, resolved by removing the sequence numbering and allowing option to use other data elements. Also, will add a note that says CHUID may need to be read to get content signer certificate to verify the signature on biometric object.
Cert-102	Certipath PMA	Judith Spencer	T	52	1639-1640	6.2	Recommend the use of PIV in environments that do not have card readers is the exception case in this guidance. OMB M-11-11 is calling for the use of the electronic features, and the FIPS should align with and support this notion.	PIV Cards are intended for use ~~can be used~~ for identity authentication in environments that are equipped with card readers ~~as well as those that lack card readers~~. Card readers~~, when present,~~ can be contact readers or contactless readers. For physical access control environments that lack card readers, the PIV card may be presented for visual examination, however, organizations should recognize the vulnerabilities associated with this practice.	Resolved by lowering the assurance level of VIS.
Cert-103	Certipath PMA	Judith Spencer	T	52	1650-1686	6.2.1	See comment 102 above. Recommend removing this section. It is not a valid use of PIV. It could be moved to an appendix, or to the end of Section 6.2, and relabeled - "Use of PIV in environments that lack card readers"	Delete Section 6.2.1	Resolved by lowering the assurance level of VIS and by moving the section towards the end. We decided not to remove or deprecate VIS because VIS is the only authentication mechanism on PIV Cards for facilities that do not have electronic PACS.
Cert-104	Certipath PMA	SPH	T	54	1694, 1722, 1737, 1809	6.2.2, 6.2.3.1, 6.2.3.2, 6.2.6	See comment 41. All discussion relating to checking card expiration should reference the (proposed) section on determining card expiration. If the PIV authentication credential has been allowed to expire and not renewed, it doesn't matter if the CHUID is unexpired, the card is invalid. This also takes care of contradictory language associated with card validity in Section 5.5 where it states that if the PIVAuth cert is revoked or expired, the card is invalid. Checking the signature on the CHUID won't get you this information, hence the contradiction.	Replace with: "Expiration and Revocation shall be checked in accord with section [???]."	Declined. We accept that some authentication mechanisms do not protect against revoked cards. Specifically update those authentication mechanisms to highlight the vulnerability.
Cert-105	Certipath PMA	Judith Spencer	E	54	1706-1711	6.2.3	Recommend this added text be made into a footnote. It is advisory in nature, seems out of place in the flow of the document, and distracts from from the issue at hand - using biometrics as an access control mechanism.	Place the text beginning: "As noted in Section 4.4,. . ." to the end of the paragraph in a footnote.	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-106	Certipath PMA	Judith Spencer	T	55	1730 & 1732	6.2.3.1 (8&9)	Why is this "FASC-N" and not "A unique identifier" as described in CHUID section above?	Recommend use of "A unique identifier" here, providing for inclusion of UUID in future iterations.	Resolved by NIST-81.
Cert-107	Certipath PMA	Bob Dulude	T	55	1730	6.2.3.1	Because of the use of a "shall" in line 1720 of this section it implies in line 1730 that the CHUID must be read to retrieve the FASC-N for the comparison check with the FASC-N in the signed biometric data block. Alternatively the FASC-N could be read from the PIV Auth certificate and compared with the FASC-N in the signed biometric data block. There are two advantages to this approach: 1) the PIV auth cert can be tied to the card via a challenge response making it more secure (note both the CHUID and Biometric data block can be copied), and 2) using the CHUID for this process could require reading the full CHUID to check its signature which will significantly increase the processing time and degrade performance. In either case the most likely implementation would have cached the signing certificate.	Since these are presumably examples and not normative prescriptions for how the various authentication mechanisms could be implemented the "shall" in 6.2.3.1 and 6.2.3.2 should be removed.	Resolved by AI-14.
Cert-108	Certipath PMA	Judith Spencer	T	55	1746 & 1748	6.2.3.2 (8&9)	See comment 106 - same question.	See comment 106 - same recommendation	Resolved by NIST-81.
Cert-109	Certipath PMA	Bob Dulude	T	56	1769	6.2.4.1	The Subject Distinguished Name (DN) is typically not required in the implementation of this authentication process. Only the unique identifier is needed.	Remove the reference to Subject Distinguished Name (DN) to eliminate confusion.	Resolved by NIST-81.
Cert-110	Certipath PMA	Bob Dulude	T	56	1772 & 1789	6.2.4.1, 6.2.4.2	The use of the phrase "Requires the use of online certificate status checking infrastructure" in the first version of this document caused considerable confusion within the industry as many people interpreted this to mean for use in "real time" revocation checking. In fact there must be a certificate status checking infrastructure but it does not have to be "online" at the time the revocation checking is done. The data can be cached.	Recommend one of two approaches: Remove the word "online" from this sentence. The word "infrastructure" says what needs to be said; or, Replace the word 'use' with 'availability'. Afterall, no one can really control how a relying party will determine risk and status checking protocol.	Accept to remove the word 'online'
Cert-111	Certipath PMA	SPH	T	57	1795	6.2.5	Current text: "...verification. A live-scan biometric..." does not mitigate YES machine behavior.	Proposed text: "...verification. A secure session is established with the card. A live-scan biometric..." May need more detail here based on secure session protocol in [SP800-73].	Declined. Section 6.2.5 (now Section 6.2.2) states the response includes information that allows the card to be authenticated. Details of how this will be accomplished will be provided in SP 800-73.
Cert-112	Certipath PMA	Judith Spencer	E	57	1795-1796	6.2.5	The sentence that begins "A live scan. . ." does not parse. There seems to be a word missing.	Suggested wording: "A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC) authentication and the card responds with an indication of the success of the on-card biometric comparison."	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Cert-113	Certipath PMA	Judith Spencer	E	57	1798-1801	6.2.5	Several editorial fixes.	The PIV Card shall include a mechanism to block this authentication mechanism after a number of consecutive failed authentication attempts as stipulated by department or agency. As with authentication using the PIV biometric, ~~alf~~ if agencies choose to implement On-card biometric comparison it shall be implemented as defined in [SP 800-73] and [SP 800-76].	Accept.
Cert-114	Certipath PMA	SPH	T	58	1839-1845	6.3.1	This table is outdated and inaccurate.	Replace with the table extracted from the FICAM AWG Federated PACS Guidance document on adjacent page.	Resolved by downgrading CHUID and VIS and by adding LITTLE or NO CONFIDENCE assurance level to Tables 6-2 and 6-3.
Cert-115	Certipath PMA	Judith Spencer	T	58	1843	6.3.1 Table 6.2	See comment 102. Remove VIS from the table as an appropriate mechanism to achieve SOME assurance. The use of VIS should be deprecated as a valid mechanism and assigned as an exception case.	Remove reference to VIS from the table.	Resolved by downgrading VIS To LITTLE or NO CONFIDENCE assurance level.
Cert-116	Certipath PMA	SPH	T	61	1927	A.5	It is anticipated that more product families will get tested, especially in light of PACS testing program growth. Current text: "The product families include…"	Proposed text: "The product families currently include…"	Resolved by ICAMSC-162.
Cert-117	Certipath PMA	SPH	E	77	2355	G.	"This version represents 5 year review of FISP 201…"	"This version represents 5 year review of FIPS 201…"	Accept.
Cert-118	Certipath PMA	SPH	E	77	2355	G.	"...received from agencies. Following is…"	"...received from agencies. Following are…"	Accept.
DAON-1	Daon	C.Tilton		6-8		2.3	The topic of this section is 'PIV Identity Proofing and Registration Requirements;' however, the content is almost entirely about the identity proofing aspect and very little about registration. The basic requirements to collect biographical and biometric data is not mentioned and deserves a bullet. [Note1 - SP800-79 is cited which contains these requirements (App G, PCI Controls and Assessment Procedures); however, the reader should not have to go to a separate document or way down into the details of this this one to find this basic requirement.] [Note2 - Use of biometrics are mentioned in 2.4 & 2.5 for renewal and reissuance, but not in 2.3 for registration.]	Add a bullet identifying the requirement to collect (or to have otherwise obtained) biographic and biometric data during registration.	Resolved by adding sections on biometric data collection, biometric data use, and chain-of-trust prior to the 'PIV Identity Proofing and Registration Requirements' section.
DAON-2	Daon	C.Tilton		6-8		2.3	The title of this section is 'PIV Identity Proofing and Registration Requirements;' and it refers to SP800-79 in the first bullet; however, it is noted that SP800-79 calls this "Enrollment/Identity Proofing". [Note - 800-79 only uses the term 'registration' when citing this section of FIPS201.]	Use the terms 'registration' and 'enrollment' consistently and/or define them to identify how they differ.	Noted. SP 800-79 will be updated accordingly.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DAON-3	Daon	C.Tilton		42		4.4	Addition of iris data to the PIV card and processes is appreciated. Because iris collection may serve 2 roles (as an alternative to fingerprint data, when it cannot be collected, and as an additional authentication method), the former use appears to receive more emphasis (despite 6.2.3).	Add a sentence somewhere that says something like: "In addition to collecting iris data when it is not possible to collect fingerprint data, agencies may choose to collect iris biometrics as a second biometric to support multimodal authentication to improve accuracy, operational suitability, to accommodate user preferrences, and/or as a backup when the primary fingerprint biometric is temporarily unavailable due to injury."	Accept in part by adding the following text: "Agencies may choose to collect iris biometrics as a second biometric to support multimodal authentication to improve accuracy, operational suitability, to accommodate user preferences, or as a backup when the fingerprint biometric is unavailable."
DAON-4	Daon	C.Tilton		42		4.4	This section allows biometric data to be transferred over the contactless interface only for on-card comparison. However, the addition of a secure channel for this purpose also provides the security necessary to enable other functions heretofor not allowable over the contactless interface; for example, PIN entry or access to biometric data for off-card comparison. [Note - Exposure of live biometric data is as useful (and in many cases more useful) to an attacker than reference data.]	Consider expanding functionality available over the contactless interface when mutual authentication and secure sessions are implemented.	Resolved by AI-7.
DAON-5	Daon	C.Tilton		42+		4.4.1	The chain-of-trust requirement is an important and appreciated addition to the standard.	None.	Noted.
DHS-1	DHS CISO	Todd Lee	T	8, 9	465-469, 514	2.4 and 2.5.1	These sections address verifying the fingerprint and iris information on the card, but omit verifying that the facial image file stored on the card is valid.	Recommend the following step be added to the issuer guidance "+ Before the card is provided to the applicant, the issuer shall verify stored digital image for both valid digital signature and fidelity of the resulting image".	Declined. The 1:1 biometric match is for the purpose of authenticating the applicant to issuer. Biometric data signature checks and fidelity checks are part of quality control procedure and are out of scope here.
DHS-2	DHS CISO	Todd Lee	T	8	472	2.4	This paragraph states that PIV card shall be valid for no more than 6 years.	The current DoD CAC and DHS PIV card validity periods are both 3 years. This validity period should be based on the agency policy/guidance. It is recommended that this paragraph be removed or changed accordingly.	Declined to remove or change the paragraph. According to FIPS 201, validity period can be based on the agency policy / guidance as long as it is not more than six years.
DHS-3	DHS CISO	Todd Lee	T	9	493	2.4.2	This sections states a grace period of 60 days for individuals that have lapsed status as federal employee or contractor	Recommend this section to be removed. OPM has not specified a grace period and this is best left to individual agencies per agency policy.	Resolved by DoD-20.
DHS-4	DHS CISO	Todd Lee	T	9	517	2.5.1	The document states that a cardholder shall be allowed to apply for a renewal starting twelve weeks prior to the expiration of a valid PIV Card. It's not necessary to specify a specific time limit for applying for a renewal card as there could be circumstances where a card needs to be renewed more than 12 weeks prior to expiration.	Recommend just requiring that the current card has not expired and not specifying a time window or leave the time window to the discretion of individual agencies.	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS-5	DHS CISO	Todd Lee	T	10	547	2.5.2	Mandatory revocation of certificates that have not been or do not have the potential for compromised will cause the overall certificate revocation lists to grow significantly without enhancing security.	Recommend change to "when the original PIV card was securely collected and properly destroyed, revocation of all certificates on the original card is optional. Otherwise, the CA shall be informed and all certificates on the PIV Card shall be revoked."	Declined. This section exclusively applies to lost, stolen, damaged, or compromised cards, which should be revoked. Renewal of card does not require revocation.
DHS-6	DHS CISO	Todd Lee	T	38	1184	4.2	This section states that a CHUID should be treated as a password, which is misleading; CHUID doesn't have the same sensitivity as password. CHUID is basically a text string that can be readily accessed, whereas a password is typically hashed or encrypted and not stored as plain text.	Recommend changing the paragraph to state what a CHUID is and what it is intended for, which is simply a static data object that can be accessed from the card and it's a unique ID that can be used by the relying systems.	Resolved by Cert-73.
DHS-7	DHS CISO	Todd Lee	T	42	1320	4.4	The document suggests that the facial image is mainly for printing on the card and for visual verification and is not necessary to be stored on the card. However, the image on the card can be altered unless it is stored on the card as a digitally signed (and thus digitally verifiable) object. A digitally signed image on the card can provide better assurance even just for visual verification.	The facial image should be incorporated on the card as one of the biometric data and as a signed object.	Accept per ICAMSC-83.
DHS-8	DHS CISO	Todd Lee	T	49	1541	5.3	The document states that CA shall issue CRLs every 18 hours, at a minimum. This parameter should be left to the agency PKI or security policy and not in this document.	Recommend removing or changing the language.	Resolved by referring to the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON] for CRL issuance requirements, including CRL issuance frequency requirements, by changing Section 5.3 from: "CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum. The contents of X.509 CRLs shall conform to Worksheet 4: CRL Profile in [PROF]." to: "CAs that issue certificates corresponding to PIV private keys shall issue CRLs as specified in [COMMON]. The contents of X.509 CRLs shall conform to Worksheet 4: CRL Profile in [PROF]."
DHS-9	DHS CSO	Brian Pittack	G					Pin Lock out: Suggests NIST provide guidance in FIPS 201-2 for remotely un-locking a PIV Card when PIN reset is required. An example would be through use of a biometric to unlock the card when presented by the PIV cardholder.	Resolved by new remote PIN reset procedure.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS-10	DHS	William.(	G	all			The thrust of the changes in this revision related to biometrics are supported by DHS. These changes are responsive to the needs for enhanced physical access control via improved functionality using the contactless interface and PIN-less operations. Inclusion of Iris modality as a fall-back to fingerprints and an option to all Departments is also a progressive revision, and is in line with movement within DHS to embrace iris modality applications.	None	Noted.
DHS-11	DHS	William.(	E	66	2016	E.1	The definition of biometrics includes the phrase "... iris scan samples...". The term "scan" can have negative implications to some readers, and can easily be avoided without loss of meaning.	Recommend to replace "iris scan samples" with "iris image samples"	Accepted everywhere.
DHS-12	DHS PLCY/SCO	Ted Sobel	E	2	261	1.3.1	Define NACI		Resolved by spelling out NACI upon first use, which is in section 2.1.
DHS-13	DHS PLCY/SCO	Ted Sobel	E	2	263	1.3.1	Define PKI		Resolved by changing PKI-PIV to PKI-CAK, which is defined in Section 6.2.4.2 (now Section 6.2.3.2).
DHS-14	DHS PLCY/SCO	James Scallan	T	8	473-477	2.4	In the "PIV Card Issuance Requirements" section there is reference to cards that contain defects. There should be some thought at NIST as to how this issue can be rectified to maintain the integrity of the PIV card.	There should be a standard for the card stock, so as to maintain the integrity of the card and its secure features.	Out of scope. Card inventory management function are out of scope of FIPS 201.
DHS-15	DHS PLCY/SCO	Ted Sobel	E	10	526	2.5.1	Define FASC-N		Resolved by spelling out FASC-N upon first use.
DHS-16	DHS PLCY/SCO	James Scallan	T	10	557-561	2.5.2	While there is reference that in "certain cases, 18 hours is an unacceptable delay," there should be a set standard for notification and cancellation that accelerates this process. Ideally, the expired credential should be terminated immediately. As most federal agencies are still meeting the challenges of using the full capability of the PIV for PACS and LACS, there is a security vulnerability (i.e. if card is used a flash pass with electronic read only) in the absence of validating a card holder's biometric.	There should be a specification encouraging immediate notification and cancellation where practical.	Declined. Procedures for de-authorizing the use of PIV Cards faster than certificate revocation information can be distributed is best left to agency discretion.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS-17	DHS PLCY/SCO	James Scallan	T	11	577-579	2.5.3	As logical access capabilities are enhanced for government systems and networks using the PIV, there are sometimes issues in the card registration process (i.e., Active Directory) when the end user has to select the most recent certificate. To avoid error and unnecessary replacement of the card, old certificates should be removed as specified by standard and/or accompanying policy.	Old certificates should be removed from the card if it is re-keyed.	Noted. While SP 800-73 permits old certificates for key management to be stored on the card in order to support decryption of data that was encrypted using the old certificates, no other old certificates can be stored within the PIV Card Application. It is very likely that some old certificates have been cached by the OS, that are not from the PIV card.
DHS-18	DHS PLCY/SCO	Ted Sobel	E	12	603	2.5.5	Define PIN		Spell out PIN on the first use.
DHS-19	DHS PLCY/SCO	Ted Sobel	E	13	643	2.5.6	Define IIF (or replace with PII)		Accept use of PII. Resolved by replacing all instances of IIF by PII. We will define PII with a reference to OMB M-07-16. Also, delete IIF from the glossary.
DHS-20	DHS PLCY/SCO	James Scallan	T	12	631-644	2.5.6	Similar to card reissuance, there needs to be a set standard to collect the card and ensure the proper systems are updated (CA notification, OCSP updates or indirect CRL publication). Does the same 18 hour standard apply for termination as it does with reissuance? Again, if so, 18 hours is a significant amount of time for a person to do damage. What is the 18 hours based on and what prohibits an issuing authority from suspending a card immediately and dispersing this information for CA action and subsequent OCSP updates or publication of CRL?	Provide a specification so that a PIV card can be fully purged from the system in a reasonable time frame, if not immediately (i.e., mitigating the risk by reducing the 18 hour window).	Declined. Text will be added to Section 2.5.6 (now Section 2.9.5) clarifying that the 18 hour standard applies. Procedures for de-authorizing the use of PIV Cards faster than certificate revocation information can be distributed is best left to agency discretion.
DHS-21	DHS PLCY/SCO	Ted Sobel	E	15	721	3.1	Capitalize "subsystem" (?)		Resolved by removing capitalization of the word 'Relying' in line 721 and 785.
DHS-22	DHS PLCY/SCO	Ted Sobel	T	17	774	3.1.2	"on the card" may confuse people between the surface and the ICC	"on the visual surface of the card"	Declined. The words "printing" and “loading” make the distinction clear.
DHS-23	DHS PLCY/SCO	Pamela Friedmann	T	21	877-892	4.1.3	Exposing the PIV card to 2000 hours of light and conducting an unspecified amount of testing for temperature and humidity, may not be sufficient for realistic use of PIV cards that are supposed to be valid for no more than six years (p. 8) and operable in a variety of climates.	Creation of specifications for cardstock that make explicit the cardstock's suitability for common and/or extreme conditions (e.g., maritime, arctic, desert, etc) over a specified period of time.	Out of scope. Cards used in extreme conditions may not last for six years and may need to be replaced more often regardless of the amount of testing done on the card. See also DHS-2.
DHS-24	DHS PLCY/SCO	Ted Sobel	T	26	1043-44	4.1.4.4	TSA does not require Gender or DOB for a PIV card.	cite an example other than TSA.	Resolved by removing the sentence, "Additional information such as Gender and Date of Birth required for Transportation Security Administration (TSA) checkpoint may also be printed as shown in Figure 4-7" in Section 4.1.4.4 (line #1043-44). Also, remove TSA reference, Gender, and DOB in Figure 4-7.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DHS-25	DHS PLCY/SCO	Pamela Friedmann	T	37	1134-1142	4.1.6.1	A digital photograph may or may not be sufficient.	For optional data elements for the PIV, suggest specifying what type of facial image is acceptable, such as 3-d facial, or other facial recognition systems using algorithms to identify key features.	Declined. The image format is specified in SP 800-76.
DHS-26	DHS PLCY/SCO	Ted Sobel	E	38	1178-79	4.2	FASC-N should already be defined by this point in the document (see comment #4)	deleted "Federal Agency Smart Credential Number"	Declined. Although FASC-N has been defined before, Section 4.2 (now Section 4.2.1) is specific to the CHUID.
DHS-27	DHS PLCY/SCO	Pamela Friedmann	G	43, 63	1346-1349	4.4.1, Appx C	On p. 43, line 1349, it states that "biometric data in the chain-of-trust shall be valid for at most 12 years", and on page 63, in the chart of "FIPS 201-2 Processes and Their Requirements", biometrics collection is considered "good for 12 years"; however, in neither instance is there any explanation for why biometrics collection should be valid for 12 years, or how this date was derived.	Explain how this date was derived.	Resolved by Cert-37. Also see DoD-52.
DHS-28	PLCY/SCO	James Scallan	T	44	1394-1414	4.4.1	What is the standard for biometric collection in the absence of a person's limbs (i.e. no hands, no eyes)? Does the access decision depend on facial image (photo comparison) or iris (if available) at this point? Also, what if fingerprints cannot be read by the scanner?	Further clarification is needed on the absence of limbs or distorted prints that prevent positive authentication of that person's identity.	Resolved by NCE-37.
DHS-29	DHS PLCY/SCO	Pamela Friedmann	T	52, 53, 54	1638-1635, 1656-1685, 1686	6.1.1-6.2.1	Although PIV cards can be used for identity authentication in environments that are equipped with card readers as well as those that lack card readers, using a visual inspection of the PIV card for access control is not secure, and reduces the PIV card's effectiveness to that of a flash-pass. Without the identity confirmation provided by a card reader, there are increased possibilities for security vulnerabilities.	Suggest recommending that card readers be used with PIV cards to maximize effectiveness.	Resolved by lowering the assurance level of VIS and by moving the section towards the end. We decided not to remove or deprecate VIS because VIS is the only authentication mechanism on PIV Cards for facilities that do not have electronic PACS.
DHS-30	DHS PLCY/SCO	Ted Sobel	E	49	1548	5.4	Define OID		Accept.
DHS-31	DHS PLCY/SCO	Ted Sobel	E	50	1585	6	Define AIA		Resolved by spelling out AIA and deleting it from the acronyms section.
DoD-0	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	G	N/A	General	0	See DoD Cover Letter for High level comments		Resolved by other DoD comments.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-1	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Critical (Technical)	N/A	General	New	FIPS 201 currently does not permit non-PIV data objects on PIV cards. This creates problems for issuers who require secure storage of organization specific, identity related data. Hosting non-PIV data on a second card application creates compatibility problems with middleware and security issues with PIN management and binding non-PIV identity data with the identity credentials on the PIV card. The only viable solution to this problem is to allow the creation of agency specific data objects within their own name space on PIV cards accessible through the standard PIV API.	Strongly recommend specifying the use of the inter-agency namespaces as outlined in NISTR 7284 to permit issuers to create organization specific data objects on PIV cards	Declined. Agency-specific applications are out of scope for HSPD-12.
DoD-2	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Critical (General)	N/A	Gen 1338	Gen 4.4.1	The concept of "chain of trust" is a significant addition to this document. As currently outlined, it requires the 10-print fingerprint scans used in the background investigation process to be secured by the PIV issuance system and compared against two live fingerprints captured by during the issuance. Most of the Federal Agencies have pre-existing, non-integrated systems for process background investigations/fingerprints to the FBI/OMB and PIV issuance, the principles outline by the "chain of trust" are not technically feasible and have significant cost ramifications. It would require PIV issuers to somehow gather the 10 prints sent to the FBI/OMB; store them with the PIV issuance system for each cardholder (in the case of DoD, for millions of people); extract 2 fingerprints from the 10; and match them. DoD is not convinced these activities provides the right mitigation to perceived vulnerability in comparison to the resources required to implement and the assets that are being protected. This should be about business decision and not security for security features sake. In these budget constraint environments, DoD MUST better understand from NIST the security value of this capability in the context of long-standing federal government processes for accessing classified information. Those processes do not require fingerprint matching and rely on the trust of security/law enforcement personnel to anchor the belief that the individual in front of them is the same individual who submitted the background investigation material and possesses the relevant clearance (i.e., "true identity" and "chain of trust"). It is not clear of the value to the federal government in create much different criteria for PIV credentials.	Strongly recommend deleting the "concept of chain of trust" or revising it to not include the requirement for fingerprints used during the background investigations process to match live scans taken in the issuance process. For biometrics, the "chain of trust" should begin with the biometrics taken during the initial PIV issuance process.	The chain-of-trust is optional. Matching of the 10 fingerprints with the 2 fingers used for on-card storage applies only when collection is done on separate visits/locations.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-3	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(General)	vi	118, 169	9 (pg. vi)	States that the standard is effective immediately. Agencies should be given time to achieve new aspects of the standard.	Recommend changing text to "Provisions of this document found in FIPS-201-1 continue to be applicable. New or changed provisions will be effective after this standard and supportive normative documents (i.e. SP800-73, SP800-76, and SP800-78,…) are approved."	FIPS 201: Resolved by the replacing Section 9 of the announcement with the following two sections: 9. Effective Date. This Standard is effective immediately and supersedes FIPS 201-1 (Change Notice 1). New optional features of this Standard that depend upon the release of new or revised NIST Special Publications are effective upon final publication of the supporting Special Publications. 10. Implementation Schedule. 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. Accreditations of PIV Card issuers (PCIs) that occur 12 months after the effective date of this Standard shall be in compliance with FIPS 201-2. FIPS 201-2 compliance of PIV components and subsystems is provided in accordance with M-06-18 [OMB0618] and M-11-11 [OMB1111] through products and services from GSA's Interoperability Test Program and Approved Products and Services List, once available. Implementation Guidance to PIV enabled federal facilities and information systems, in accordance to M-11-11 will be outlined in the "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance." --- Note: The aspects of FIPS 201-2 that are specified as mandatory to implement are already fully specified, as none of the new capabilities in FIPS 201-2 are specified as mandatory to implement. Thus, the mandatory requirements of FIPS 201-2 can be implemented without waiting for the related special publications to be updated. Requirements that are mandatory in FIPS 201-2, but that were optional in FIPS 201-1, do not have to be implemented immediately upon approval of FIPS 201-2, but must be implemented in accordance with the timetable that will be provided by OMB, regardless of when the related special publications are updated.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-4	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	2	258	1	A roadmap and an estimated timeline for the continual upgrade of security protocols will allow both the government and the private sector to estimate the cost of future requirements allowing them to plan accordingly.	Recommend inserting the following paragraph: "We will develop a future focused roadmap and an estimated timeline for changes in security requirements with the hope of allowing agencies and industry to better prepare for upcoming requirements."	Declined. OMB will provide timelines and further information for planning purposes. See also DoD-3.
DoD-5	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	3	287	1.3.5	There is no information on adoption/migration between versions of FIPS 201.	There needs to be a new special publication that specifies adoption practices for the incremental updates of FIPS 201. FIPS 201-2 should reference this document. Specifically, this new SP should cover sunrise and sunset processes, especially in relation to Sections 1.3.3 and Section 1.3.4.	Resolved by Cert-5.
DoD-6	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(General)	1	230	1	Although we agree with the removal of PIV-I and PIV II from the document, and agree that requirements for PIV-Interoperable should be detailed in the FBCA CP, FIPS-201 should include accommodations for agencies who have implemented electronic validation and who can register PIV-Interoperable credentials and link them to successful completion of a NAC-I to allow their affiliates who have PIV-Interoperable credentials to use them instead of having to issue a PIV card.	Recommend adding the following text to Section 1.2, "Federal agencies who have processes in place to electronically authenticate credentials that have been issued by providers certified by the Federal PKI Policy Authority as compliant with the PIV-Interoperable standard (add footnote to PIV-I for NFI link http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf) may register PIV-I credentials in lieu of PIV credentials provided that access attributes such as successful completion of a NAC-I can be also be electronically validated."	Declined because HSPD-12 specifies "... secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)." The use of externally issued PIV-I credential as a replacement for the PIV card, therefore, is not the intention of HSPD-12.
DoD-7	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	3	288 - 291	1.3.5	The versions should be tied to specific releases of FIPS201 or appropriate NIST Special Publications. Also, text lacks specific requirements for when to introduce new version number. Specific text: "New version numbers may be assigned in [SP 800-73] depending on the nature of the change. For example, new mandatory features introduced in a revision of this standard, may necessitate a new PIV card application version number so that systems can quickly discover the new mandatory features. Optional features, on the other hand, may be discoverable by an on-card discovery mechanism."	Recommend specifying types of changes that require new version number. I.e.: "New version numbers may be assigned in [SP 800-73] depending on the nature of the change. For example, all requirements changes in this standard or supporting specifications that require software changes to the card data model, or card edge or to the APIs (i.e. SP800-73 Part 3) shall be assigned a new version number. In addition, new mandatory features..."	Resolved by Cert-6. Consider also that FIPS 201 documentation (SPs) will specify the reasons for a new version number if and when the new version number is needed. Section 1.3 is only explaining a Change Management principle that will rule a version number change.
DoD-8	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	5	358	2.1 First bullet (+) in second series	Remove “true” in referenced sentence, “Credentials are issued 1) to individuals whose true identity has been verified.” The overall goal in long-standing Federal investigative processes and in FIPS 201 identity proofing is to authenticate the claimed identity of the applicant. To verify true identity adds the burden to conduct 1:N biometric matching against entire PIV population in the issuance and management system.	Recommend changing the text to "Credentials are issued 1) to individuals whose identity has been verified and 2) after a proper authority has authorized issuance of the credential;"	Resolved by deleting the word "true". Also in the definition of "identification" in Appendix E.1 (now Appendix C.1), remove the word "true".

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-9	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	6	377	2	Section references guidance from a specific memo with a specific date, requiring agencies to go hunt it up, wouldn't it be easier to just include the guidance within FIPS 201 itself?	Recommend incorporating specific applicable requirements from the Springer memo that are not already included into section 2.2 of the FIPS-201 revision.	Declined. It is not specified what sections to incorporate. The Springer Memorandum will be likely superseded by OPM's future tiered investigative standard. Memoranda could be amended. Including these memoranda (or part of it), therefore is not advisable.
DoD-10	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Editorial)	6	382	2	The last bullet in this section talks about chain-of-trust, but this concept has not yet been introduced and no description is provided here.	Recommend defining chain-of-trust before it is used here.	Resolved by AMAG-6.
DoD-11	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	6	386 - 389	2.3/Bullet 2	The second bullet in section 2.3 [on NACI, NCHC, etc.] should be cut and incorporated into section 2.2 on Credentialing Requirements. This is part of the "credentialing determination" process and can be linked to the identity proofing and registration via the chain of trust as described further in the section.	Recommend moving 2nd bullet to 2.2 and change to: "The credentialing process shall begin with initiation of a NACI or equivalent. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI. Also, the FBI NCHC (fingerprint check) shall be completed before PIV issuance. Appendix B, Background Check Descriptions, provides further details on NACI."	Declined. This is in line with the Springer memorandum, which describes the content of bullet #2 as part of the credentialing process.
DoD-12	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	6	399 - 405	2	Question 1: What is the fundamental difference between documents in bullet 5 and 6? Question 2: Why was the DoD CAC specifically specified over other Federal PIV Cards?	Recommend clarifying the difference in accepting I94 vs. I94A with passport. Also, clarify if NIST was attempting to specify a DoD CAC population (Military).	Resolved by replacing the Common Access Card with the PIV Card on the list.
DoD-13	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (General)	7	412	2	The secondary identity source document are not the most fraud/tamper resistant credentials or verifiable in most case. As such, departments/agencies should have the ability to restrict or expand to meet their business needs.	Strongly recommend providing flexibility for the Federal Agency by adding, "Federal Departments or Agencies can further restrict or expand the secondary identity source documents as deem necessary."	Resolved by noting that the list of identity source documents may be more restrictive.
DoD-14	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Editorial)	7	438	2.3/Bullet 5	For clarity, remove or modify the reference to "issuance" within 2.3 since this section is focused on identity proofing and registration (issuance is in 2.4). Also, other processes (credentialing, reissuance, renewal) apply in this case.	Recommend changing 5th bullet to: "The PIV identity proofing and registration process, when combined with the remaining PIV processes, shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person."	Accept to include renewal and reissuance. Specifically mentioning "issuance, reissuance, and renewal" vs. 'other processes' adds clarity.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-15	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (General)	7	442 - 444	2	The last paragraph on page 7 states, "The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head of the Federal department or agency." Requiring this level of senior management endorsement within a Federal Department or Agency is unnecessary and repetitive to C&A activities outlined in SP 800-79-1.	Strongly recommend changing to, "The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as outlined in SP800-79-1."	Resolved by adding the underlined text as follows: The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head or deputy secretary (or equivalent) of the Federal department or agency.
DoD-16	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (Technical)	8	445	2.3/ Last Paragraph pg. 8	Change last paragraph of this section to more specifically address the requirements for identity source documentation for citizens of foreign countries. The rationale is that the current language indicates that the requirements listed "also apply to citizens of foreign countries." However, it only goes on to state that a registration and approval process must be established – the paragraph does not address the fact that the requirement listed (specific list of source documents for primary and secondary documentation) cannot be applied to these individuals in all cases. Due to international agreements with host nations, citizens of foreign countries working for the Federal government may not have / be required to possess identity source documents from the I-9 list. Furthermore, the reference that the "identity proofing" requirement applies to foreign citizens, but a process for "registration and approval" must be established by other means is confusing. "Approval" should no longer be attributed to this section as it is addressed in the new 2.2 Credentialing Requirements section.	Strongly recommend changing paragraph to: "The requirements for identity proofing and registration also apply to citizens of foreign countries who are working for the Federal government overseas. However, a process for identity proofing and registration must be established using a method approved by the U.S. Department of State's Bureau of Diplomatic Security, except for employees under the command of a U.S. area military commander. These procedures may vary depending on the country."	Accept.
DoD-17	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (Technical)	8	461- 469	2	This section states, "biometric match requires either a match of fingerprint(s) or a match of iris image(s)."	Strongly recommend the references to "iris image(s)" be deleted or changed to "...match of fingerprint (s), optionally match iris image (s) or review of facial image." This aligns with current required/deployed technology within the PIV issuance process without requiring additional, cost prohibited investments.	Resolved by the text introduced by DOT-11.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-18	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Editorial)	8	457 - 460	2.4/Bullet 3/Page 8	The bullet reiterates the investigative requirements – each times these requirements are mentioned the wording is slightly modified. Suggest changing the bullet to more directly tie the requirement to one place (Section 2.2 that was added for Credentialing Requirements)	Recommend changing bullet to: "The process shall ensure that the credentialing requirements have been met in accordance with Section 2.2. The PIV Card shall be revoked if the results of the credentialing determination so justify." The second bullet of section 2.3 should also be moved to Section 2.2 so that the credentialing determination/investigative requirements are in one location.	Resolved by DoD-11.
DoD-19	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	8	473	2	The statement "Cards that contain typographical defects, contain errors in optional fields, are not properly printed, or are not delivered to the cardholder are not considered PIV Issued Cards." Not sure this is a good idea from a security standpoint. If the card was intended to be issued as a PIV card, it should be treated as a PIV card. If there are errors on the card, it should be revoked, but all requirements connected with the management of the card and the revocation of it should be followed.	Recommend deleting the reference or clarifying the intent of addressing cards with defects.	Resolved by Cert-18.
DoD-20	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	9	492	2.4.2	This sections outlines a grace period of 60 days.	Recommend this be removed. OPM is the Suitability Executive Agent per EO 13467, and is responsible for reciprocity policy. OPM has not specified a grace period and more than likely has left that up to the Agencies. A "not more than 2 year" break in service has been used for National Security and Suitability "grace periods."	Accept.
DoD-21	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	9	507	2.5.1	Why specify a time limit for applying for a renewal card? There could be circumstances (individual is going to be deployed to a remote location) where it makes sense to renew a card more than 12 weeks prior to expiration.	Recommend just requiring that the current card has not expired and not specifying a time window.	Resolved by DHS-4.
DoD-22	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	9	515	2.5.1	The last sentence of the paragraph indicates that "The entire identity proofing and registration process is required if a cardholder's chain-of-trust record is not available." This should be modified to allow the Agency to determine the extent to which the process will be repeated for those cases where a 1:1 biometric may not be possible. Otherwise, each Agency may be unnecessarily conducting NCHCs and NACIs to accommodate this requirement for individuals with valid checks on file.	Recommend changing the last sentence to "The initiation of an approved identity proofing and registration process is required if a cardholder's chain-of-trust record is not available."	Resolved by adding alternative mechanism to reconnect to chain-of-trust. In addition, even in cases in which the entire identity proofing and registration process needs to be repeated, there is no requirement to conduct an NCHC or background investigation if a "completed and successfully adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation record" can be located and referenced.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-23	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Editorial)	11	568-569	2.5.2.1	The first three sentences of this section seem to be trying to express a single idea which can be concisely stated.	Recommend changing to "Name changes frequently occur as a result of marriage, divorce, or as a matter of personal preference."	Accept.
DoD-24	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	10	542	2.5.2/	The last sentence of the paragraph indicates that "The entire identity proofing and registration process is required if a cardholder's chain-of-trust record is not available." This should be modified to allow the Agency to determine the extent to which the process will be repeated for those cases where a 1:1 biometric may not be possible. Otherwise, each Agency may be unnecessarily conducting NCHCs and NACIs to accommodate this requirement for individuals with valid checks on file.	Recommend changing the last sentence to "The initiation of an approved identity proofing and registration process is required if a cardholder's chain-of-trust record is not available."	Resolved by DOT-15.
DoD-25	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	10	547	2.5.2	Mandatory revocation of certificates that have not been or do not have the potential for the private key to be compromised only causes certificate revocation lists to grow and does not enhance security. And any time there is a potential for compromise of the key the certificate needs to be revoked. Stating that the certificate is revoked by placing the serial number on the CRL - really not a necessary statement - that is what the standard for CRLs calls for.	Recommend changing from " The CA shall be informed and the certificates corresponding to the PIV Authentication Key and asymmetric Card Authentication Key on the PIV Card shall be revoked. Revocation of the Digital Signature Key certificate is only optional if the PIV Card has been collected and zeroed or destroyed. Similarly, the Key Management Key certificate should also be revoked if there is risk that the private key was compromised. Certificate revocation lists (CRL) issued shall include the appropriate certificate serial numbers." to "If the PIV Card has been collected and is securely handled until zeroed or destroyed, revocation of all certificates on the card is optional. Otherwise, the CA shall be informed and all certificates on the PIV Card shall be revoked."	Resolved by DHS-5.
DoD-26	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Critical (General)	11	595 - 956	2.5.4	This bullet states, "the PIV Card will communicate with no end point entity other than the PIV Card issuers during the remote post issuance update." DoD can envision the use of multiple Global PlatformTM domains on a single PIV in which the applications within the PIV domains would be managed by the PIV issuer and the application within a secondary domain may be managed directly by the owner of the line of business the domain is supporting. All of which would not weaken the overall security or integrity of the PIV credential.	Strongly recommend deleting the next to last bullet or adding text restricting this requirement by each GP security domain rather than the entire PIV credential.	Revise the bullet as follows: "The PIV Card Application will communicate with no end point entity other than the PIV Card issuer during the remote post issuance update."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-27	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (General)	11	596 - 598	2.5.4	The last bullet within this section states, "If the PIV Card post issuance update begins, but fails for any reason, the PIV Card issuer shall immediately terminate the PIV Card as described in Section 2.5.6, and a diligent attempt shall be made to collect and destroy the PIV Card." This excerpt prescribes entirely too much about the potential implementations of post issuance capabilities by the PIV issuers. DoD has supported remote post issuance updates of CAC and CAC PIVs since 2002. DoD can envision technically sound and secure ways to reprocess failed transactions without invalidating credentials. Remote post issuance transactions connected to our issuance system are susceptible to delays in communications that may cause a transaction to fail. This shouldn't automatically require the card to be terminated. There are other available techniques to ensure the integrity of remote post issuance transactions and CAC PIV.	Strongly recommend deleting this bullet. This level implementation details must be left to the PIV issuer to determine.	Accept to delete last bullet.
DoD-28	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Editorial)	26	739	3	Graphic unnecessarily rotates text boxes within the "PIV Card Issuance and Management" box of the graphic making the example harder for the reader to grasp at a glance.	Recommend rotating the text boxes within image so that it is readable within the normal orientation of the page. Text boxes can be stair stacked with gaps between if necessary.	Accept.
DoD-29	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Editorial)	28	805	3	Graphic shows a single exit path from the text box "PIV Card Maintenance" with two landing points making the logical flow of the paths ambiguous.	Recommend annotating the differentiator between these paths.	Resolved by adding annotation for each path.
DoD-30	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (Technic al)	20	833	4.1.6.1, 4.4, and 4.4.1	Draft FIPS 201-2 appears to outline iris biometrics as an optional feature, however when discussing biometric contingencies if two fingerprint biometrics are unavailable, it requires the use of iris biometrics. These differences must be addressed so that iris biometrics are optional and facial images continue to be the secondary biometric. A required migration to iris within the CAC/PIV issuance process would be unaffordable within DoD.	Strongly recommend making the collection of iris images optional for all processes.	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-31	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	20	833 - 1122	4.1.1 thru 4.1.5	Card topology specifications are split between FIPS 201-2 and SP 800-104	Recommend moving all physical card and topology definitions (specifically sections 4.1.1 thru 4.1.5) into SP800-104 and make this a normative reference from FIPS 201-2.	Resolved by moving information from SP 800-104 to FIPS 201-2 and making Zones 15F and 18F mandatory. Also, withdraw SP 800-104.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-32	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (General)	21	893 - 896	4.1.3	The bullet "Department and agencies shall ensure that the card meets the requirements of Section 508 of the Rehabilitation Act" is too broad for the purposes of this standard and should be deleted. It assumes that there are specific requirements in the act that can be attributed to PIV cards when, in fact, Section 508 is about the bigger issue of overall "access to and use of information and data" for individuals with disabilities. Attempting to outline a broad requirement specific to the physical topology of a PIV card does not take into account the case by case nature in which Section 508 compliance shall be addressed by each Agency.	Strongly recommend deleting the bullets on the broad requirement for 508 compliance. If a reference to 508 is still required delete bullet 5 and modify bullet 8 to read as follows: "Decals shall not be adhered to the card unless specifically required by an Agency to assist with compliance of Section 508 of the Rehabilitation Act. If a decal is used in this case (for example, an adhesive Braille letter) it shall be place in Zone 21F as defined in Section 4.1.4.3."	Resolved by removing reference to Section 508 in bullets 5 and 8. In addition, the following statement was added to Section 8 of Announcement: "In implementing PIV systems and pursuant to Section 508 of the Rehabilitation Act of 1973 (the Act), as amended, agencies have the responsibility to accommodate federal employees and contractors with disabilities to have access to and use of information and data that is comparable to the access to and use of the information and data by federal employees and contractors who are not individuals with disabilities. In instances where Federal agencies assert exceptions to Section 508 accessibility requirements (e.g., undue burden, national security, commercial non-availability), Sections 501 and 504 of the Act requires Federal agencies to provide reasonable accommodation for federal employees and contractors with disabilities whose needs are not met by the baseline accessibility provided under Section 508. While Section 508 compliance is responsibility of Federal agencies and departments, this Standard specifies options to aid in implementation of the requirements: + Section 4.1.4.3 specifies Zones 21F and 22F as an option for orientation markers of the PIV Card. + Section 2.8 describes an alternative to the National Criminal History Check (NCHC) in instances where an applicant has unclassifiable fingers. + Sections 2.8, and 2.9 specify alternative methods for 1:1 biometric match required at PIV card issuance, reissuance, renewal, and reset. + Section 6 defines authentication mechanisms with varying characteristics for both physical and logical access (e.g., with or without PIN, over contact, contactless, or virtual contact access)." Replace bullet 5 with "There are methods by which proper card orientation can be indicated. Section 4.1.4.3, for example, defines Zones 21F and 22F, where card orientation features may be applied. Note: If an agency determines that tactilely discernible markers for PIV Cards imposes an undue burden, agencies must implement policies and procedures to accommodate employees and contractors with disabilities in accordance with Sections 501 and 504 of the Rehabilitation Act."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-33	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technic al)	23	Table 4.01	4.1.4.1	Paragraph 4.14.1 describes truncated names in a note but Figure 4-1 does not give an example.	Recommend adding an example of a name that has been truncated with 7 point font.	Resolved by adding an example of a long name that is truncated in Table 4-1.
DoD-34	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (Technic al)	24	973	4.1.4.2	4.1.4.2 Mandatory Items on the Back of the Card. The orientation of the back of the card has been changed from FIPS201-1 requirements. Hopefully the authors intended the engineering diagrams (which have been changed from the current FIPS 201 version) to indicate a view of the printing on the back of the card as seen through a transparent front. If that is not the case, these changes to the topography would have a significant impact to DoD's manufacturer's process. Such as: - What is shown would represent a departure from the ISO standard placement of the mag stripe. This custom change to the process for the PIV CAC would likely result in higher changeover and recurring manufacturing costs, and perhaps higher material costs. - Changing the position of the magnetic stripe from the right to the left side of the card (as shown in figure 4.7 on page 34) would require a manufacturing process change to deploy. The mag stripe is embedded in one of the bottom layers of the card when the card layers are fused together during production. - Changing the orientation or the side on which the serial number of the card is laser engraved would likewise cause a change in the manufacturing process. - Changes to the placement of the mag stripe and data fields on the back side would also result in post-production printing process and material changes. The over-laminate used to protect the printing on the backside would have to be changed to protect different fields and not interfere with the new placement of the mag stripe.	(if this is an engineering diagram indicting a view of the printing on the back as seen through a transparent front) Strongly recommend the diagram be marked according to the standards of that convention and should then be labeled as such . If the view intent is correct (same as in FIPS201-1), then DoD recommends clarifying the intent of the diagrams and making modifications to bring them back in line with the current FIPS 201 standard.	Resolved by reverting back to FIPS 201-1, removing references to TSA, DOB, and Gender, adding 'B' to zone numbers. Removed reference to TSA as per resolution on comment number DHS-24.
DoD-35	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substanti ve (Technic al)	26	1023	4.1.4.3/ Zone 18F/pa ge 26	The wording describes the Affiliation Color Code in “normative” language as opposed to being an optional feature.	Recommend changing the Zone 18F wording to emphasize optional nature by added “If used, the affiliation color code “B” for Blue,…” etc.	Resolved by DoD-31.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-36	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Substantive (Technical)	37	1133	4.1.6.1	The proposed use of the CAK solely as an additional single factor authentication method is an inefficient use of card resources. In addition to interoperable PACS authentication, there is a need for encryption and privacy of the contactless interface and mutual authentication to establish trust with a terminal. Within DoD, the implementation of the CAK will increase card issuance time and user experience.	Recommend defining the CAK and minimum additional keys and associated authentication mechanisms to support efficient PACS authentication (including mutual authentication) and secure contactless interface. Until these mechanisms are fully defined, the CAK should remain optional.	Resolved by Cert-80. Note: Since the CHUID will be deprecated due to low identity assurance (little to none), the CAK will be the only mandatory one-factor authentication mechanism over the contactless interface that isn't deprecated.
DoD-37	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(General)	37	1143	4.1.6.1	The change in language will not create undo requirements on industry and federal agencies but will rather provide guidelines for these partners to make appropriate enhancements while maintaining interoperability.	Recommend inserting at the end of the sentence the following, "should it be considered where necessary."	Declined. Proposed change implies SP 800-73 does not currently contain other data elements but SP 800-73 does (e.g., CCC and Security Object).
DoD-38	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	37	1153	4.1.7	The statement "The PIV Card shall be activated to perform privileged operations such as reading biometric information…" may not be applicable in the event that On-Card Biometric Comparison is implemented. This requires further clarification.	Recommend changing statement to "The PIV Card shall be activated to perform privileged operations such as reading biometric information (in support of Off-Card Biometric Comparison)…"	Resolved by revising the sentence to "The PIV Card shall be activated to perform privileged operations such as using the PIV Authentication key, digital signature key, and key management key." Note that reading biometric information from the card implies reading the off-card biometric data. OCC reference data is not exportable.
DoD-39	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Editorial)	37	1159-1162	4.1.7.1	Concerning the statement "PIV Cards shall implement user-based cardholder activation to allow privileged operations using PIV credentials held by the card. At a minimum, the PIV Card shall implement PIN-based cardholder activation in support of interoperability across departments and agencies. Other card activation mechanisms, only as specified in [SP 800-73], may be implemented and shall be discoverable.", is the expectation that the On-Card Biometric Comparison will enable privileged operations (such as releasing the private key)?	Consider specifying an example of another activation mechanisms, such as On-Card Biometric Comparison.	Accept by replacing: "Other card activation mechanisms, only as specified in [SP 800-73], may be implemented and shall be discoverable." with "Other card activation mechanisms (e.g., OCC card activation) only as specified in [SP 800-73] may be implemented and shall be discoverable.
DoD-40	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	38	1177	4	The statement that a CHUID should be treated as if it were a password doesn't make sense. The CHUID is significantly less secure than a password. A password is not supposed to be written down or recorded, but a CHUID can be obtained from anyone with a contactless reader and proximity to the card.	Recommend replacing the current text with the following, "The CHUID may be read and used by the relying systems, but it should be treated as an identifier only for purposes of authentication and retention. Because the CHUID is a static data object which can be read from the card, the CHUID is not considered resistant to cloning; it can be copied and used to gain access."	Resolved by Cert-73.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-41	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	38	1178-1181	4	This should define explicitly what the mandatory and optional data elements are in the CHUID. The UUID must be mandatory for interoperability between PIV and PIV-I ecosystems. The details of formatting should be specified in [SP800-73], not in FIPS 201.	Recommend replacing the paragraph with this proposed text: "The PIV Card shall include the CHUID as specified in [SP800-73]. The following fields are mandatory in the CHUID: - FASC-N - GUID - Expiration Date - Issuer Asymmetric Signature"	Resolved by making the UUID in the GUID field mandatory.
DoD-42	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Editorial)	40	1244	4.3	The bullets on this page should be consistent about discussing PIN activation and interface availability.	A table would be helpful with columns: key name, key type (symmetric, asymmetric), activation (not required, unlock, per transaction), interface (contact, contactless, both).	Resolved by DoD-43 and DoD-44 since now the text is consistent about discussing PIN activation and interface availability. Additional details about each key including access to keys are addressed later in the same section.
DoD-43	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Substantive (Technical)	40	1245	4	Document states, "The PIV authentication key shall be an asymmetric private key that is accessible from the contact interface…" The private key itself is not accessible.	Recommend changing the text to "The PIV authentication key shall be an asymmetric private key that supports card authentication for an interoperable environment via challenges and signed responses via the contact interface."	Resolved by replacing: "The PIV authentication key shall be an asymmetric private key that is accessible from the contact interface and supports card authentication for an interoperable environment." with "The PIV Authentication key is a mandatory asymmetric private key that supports card and cardholder authentication for an interoperable environment." Additional details about each key including access to keys are addressed later in the same section.
DoD-44	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Substantive (Technical)	40	1248	4	Document states, "The asymmetric card authentication key shall be a private key that is accessible over the contactless and contact interface and supports card authentication for an interoperable environment." The private key itself is not accessible.	Recommend changing the text to "The asymmetric card authentication key shall be an asymmetric private key that supports card authentication for an interoperable environment via challenges and signed responses via the contactless and contact interfaces."	Resolved by replacing: "The asymmetric card authentication key shall be a private key that is accessible over the contactless and contact interface and supports card authentication for an interoperable environment." with: "The asymmetric Card Authentication key is a mandatory private key that supports card authentication for an interoperable environment." Additional details about each key including access to keys are addressed later in the same section.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-45	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Substantive (Technical)	40	1252	4	The symmetric key can be used through either interface (contact or contactless). If so, it should be stated.	Recommend adding the following text "The symmetric card authentication key can be used via either the contactless or contact interface."	Declined. Additional details about each key including access to keys are addressed later in the same section.
DoD-46	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Substantive (Technical)	40	1253	4	State that the digital signature key is used only with the contact interface	Recommend adding the following text "The digital signature key is an asymmetric private key supporting document signing via the contact interface …"	Declined. Additional details about each key including access to keys are addressed later in the same section.
DoD-47	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Substantive (Technical)	40	1255	4	State that the key management key is used only with the contact interface.	Recommend adding the following text "The key management key is an asymmetric private key supporting key establishment and transport via the contact interface, and it is optional.	Declined. Additional details about each key including access to keys are addressed later in the same section.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-48	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Critical (Technical)	41	1276	4	Change the following text: "Issued PIV Authentication certificates shall also include a PIV NACI indicator extension, until such time that OMB approves a government-wide operational system for distribution of Background Investigation status information (see Section 2.5). OMB is working on OMB a government-wide operational system for distribution of Background Investigation status information (see Section 2.5). When such a system becomes operational, relying parties will be required to check that system as part of access control decisions." Since the original draft FIPS 201 of 2004, DoD has outlined its concern with the requirement to include a cardholder's background investigation status within fields of the PIV authentication certificate. DoD has been concerned with how this information would be updated to provide accurate information to relying parties and the omission of existing ways organizations verify background investigations. Our philosophy has been to facilitate the exchange of this information across agencies through backend attribute exchange transactions between cards issuers, if needed. During the summer 2009, members of the Federal CIO Council's Identity Credentialing and Access Management Sub-committee (ICAM SC) agreed to remove the NACI indicator requirement from future revisions. This agreement should be reflected in FIPS 201-2.	Strongly recommend deleting NACI requirement or changing text to "Since agencies are not updating the NACI indicator in certificates after a person's investigation has been completed and some agencies, including DoD do not include the NACI indicator, the NACI indicator is now optional and deprecated. OMB approves such an operational system, the inclusion of the PIV NACI indicator extension in issued PIV Authentication certificates is optional and deprecated."	After discussions with OMB, the NACI indicator requirements will remain as previously specified in FIPS 201-1 and in M-05-24. The second draft of FIPS 201-2 will be changed accordingly to reflect this. Also: Given the new investigative standard, we will replace all occurrences of 'NACI indicator' with 'NACI indicator (background investigation indicator)'
DoD-49	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	42	1318	4	No mention is made as to what quality the biometric data must adhere and a full set of prints is not defined.	Recommend describing what is meant by a full set of fingerprints (rolled/slapped) and the standard that will be used for biometric information quality assurance.	Resolved by adding the following sentence to Section 2.3: Fingerprint collection shall be conformant to the procedural and technical specifications of [SP 800-76].
DoD-50	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	42	1327	4	It is not clear what the meaning of "biometric comparison data" is.	Recommend defining or explaining this term.	The term "on-card biometric comparison data" will be replaced with "fingerprint templates for on-card comparison".

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-51	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Substantive (Technical)	42-44	1386-1396	4.4.1	Facial image matching--Section 4.4.1 stipulates that facial images will be used for manual/visual matching only. We have a specification already in force and reliable automated facial matching in controlled environments. DoS has a major facial recognition program for use in their VISA application process, and DoD routinely conducts facial matching. Given that matching algorithms are expected to continue to mature, why not leave the possibility in the standard for automated recognition?	Recommend adding a new main bullets that states, "For optional automated matching of facial image within PIV reissuance processes and guard workstation to authenticate cardholders."	See text revised per ICAMSC-83.
DoD-52	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	Substantive (Technical)	43	1349	4.4.1	Time limit for valid biometrics. Does this time period assume that no operations, diseases, or injuries have occurred that may significantly alter one's biometrics?	Recommend delineating the basis for considering collected biometrics valid for 12 years	Resolved by disposition of Cert-37. [The basis for the 12 year number is weak absent long term studies; biometric verification accuracy will degrade as a slowly varying continuous function of time elapsed between enrollment and verification. Effects are traditionally mitigated via re-enrollment.].
DoD-53	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	43	1350-1351	4.4.1	The statement "A card issuer shall be able to import and export a chain-of-trust in the manner of representation described in [TBD]." Where is TBD defined?	Recommend clearing up the "TBD."	Resolved by citing [SP 800-156] and adding the proper entry to the bibliography.
DoD-54	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	43	1385	4.4.1/Note 13	The Note 13 on the chain of trust puts too much emphasis on the 1:1 biometric check given the realities of current PIV operations (failure to acquire/match for fingerprints). The note, as written, could result in unnecessary background check processes on top of an already burdened system. The references to the chain of trust should be reworked throughout the document to allow each Agency to reconnect a chain of trust with a process that also consider other factors when a 1:1 biometric match cannot be completed.	Recommend deleting note 13 and re-emphasize throughout that each Agency will utilize an approved identity proofing and registration process in the cases in which the chain-of-trust cannot be reconnected with a 1:1 biometric match.	Accept to delete footnote 13. Also permit the use identity source documents for verify an individual's identity in cases in which a 1:1 biometric match cannot be performed.
DoD-55	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Technical)	47	1500	4.5.4	The statement "If the PIN input device is not integrated with the reader, the PIN shall be transmitted securely and directly to the PIV Card for card activation." does not contain guidance for desktop computers.	Recommend adding, "Desktop computers used with a PIV and card reader shall undergo frequent automatic scans for viruses and other malware to prevent capture and disclosure of the PIN."	Resolved by adding the following text to Section 4.4.4 (formerly Section 4.5.4), Card Activation Device Requirements. "Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document." Add reference to SP 800-53.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-56	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	48	1527	5.2.1	Reference is made to [PROF] for the certificate profiles. It is unclear why an LDAP URL is required for the Card authentication profile whereas legacy PKIs were exempted from LDAP for the PIV Authentication certificate. LDAP is blocked within DoD and cannot readily take advantage of caching.	Recommend changing the text to "…conform to Worksheet 8:…in [PROF]; except that the requirement for LDAP URLs is deprecated."	Since Worksheet 8 in the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF] was specifically written to specify the requirements for the Card Authentication Certificate, we believe this comment is best address by modifying [PROF] rather than by changing the referenced line in FIPS 201-2.
DoD-57	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	49	1541	5	"PIV private keys shall issue CRLs every 18 hours, at a minimum." 18 hours is not conducive to issuing at a fixed time daily.	Recommend backing off to 24 hours.	Resolved by DHS-8.
DoD-58	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	49	1545 - 1549	5	Change the following paragraph: "PIV Authentication Certificates and Card Authentication Certificates issued by legacy PKIs shall meet the requirements specified in Section 5.2.1. Departments and agencies may assert department or agency-specific policy OIDs in PIV Authentication Certificates and Card Authentication Certificates in addition to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively." During the SHA-2 transition and use of new policy OID, we have discovered that asserting policy OID from one domain removes the flexibility for both sides of cross certified domain. It is desirable to map the policies to provide requisite security and flexibility to cross-certified domains. For the policy assertions to work securely, the applications should process policies and policy mapping appropriately and not just pick the policy in the end certificate. Thus, mapping to appropriate policies (as opposed to direct assertion) will provide requisite security while maintaining flexibility.	Recommend changing to: "PIV Authentication Certificates and Card Authentication Certificates issued by legacy PKIs shall meet the requirements specified in Section 5.2.1. Departments and agencies may assert department or agency-specific policy OIDs in PIV Authentication Certificates and Card Authentication Certificates and map these OIDs to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively or may directly assert the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively."	FIPS 201-1 required all PIV Authentication certificates issued on or after January 1, 2008, to assert a policy OID from the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON]. Since PIV Authentication certificates may be valid for at most three years, at this point all unexpired PIV Authentication certificates should assert a policy OID from [COMMON]. Since FIPS 201-1 was first published, the Federal PKI Policy Authority (FPKIPA) has made changes to [COMMON] in order to accommodate the needs of Legacy PKIs, where possible, while maintaining conformance to FIPS 201 and its related Special Publications. Changing FIPS 201-2 at this point to allow Legacy PKIs to assert department or agency-specific policy OIDs in authentication certificates instead of the policy OIDs from [COMMON] would reduce interoperability since relying parties would no longer be assured that there is a common baseline of requirements against which all authentication certificates on PIV Cards are issued.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-59	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	49	1566	6	Document states, "CAs that issue authentication certificates shall maintain an LDAP directory server that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it." LDAP is blocked by DoD and does not readily support caching. Recommend making HTTP 1.1 the standard and deprecating LDAP.	Recommend the CAs that issue authentication certificates shall maintain a repository that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it. The repository shall make CRLs available via HTTP 1.1 and may optionally support LDAP during a transition period. LDAP is deprecated.	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.
DoD-60	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	49	1573	5.5.1	The document says, "This standard requires distribution of CA certificates and CRLs using LDAP and Hypertext Transport Protocol (HTTP)." LDAP should be deprecated.	Recommend changing text to "This standard requires distribution of CA certificates and CRLs using Hypertext Transport Protocol (HTTP). LDAP is permitted as well, but is deprecated."	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.
DoD-61	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (General)	50	1576 - 1581	5.5.1	This section appears to infer any x.509 public key infrastructure (asymmetric cryptography) certificate that contains the FASCN or some representation of the FASCN cannot be make publically available. This requirement makes no sense when trying to use PKI as intended and supporting interoperability/cross recognition of PKI certificates amongst federal issuers. Public certificates must be public. It is not clear what the concern may be with the FASCN as part of the CHUID being within a public certificate, when the CHUID is a free read on contact and contactless interfaces of the PIV.	Strongly recommend deleting this requirement.	Declined. This restriction is in place for privacy reasons. It does not limit distribution of the certificates by the cardholder, nor does it prevent limited distribution of the certificates by departments and agencies. It also does not preclude caching of certificates by relying party systems for local use. Furthermore, the restriction only applies to certificates that contain the FASC-N, which typically means only the authentication certificates. In most cases, authentication certificates are provided to the relying party at the time of use. Key management certificates, which are most appropriate for distribution via publicly accessible repositories do not typically include the FASC-N, in which case they would not be covered by this restriction.
DoD-62	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Editorial)	55	1734	6.2.3.2	Since the attended authentication of PIV Biometric is nearly the same as unattended, the difference should be highlighted rather than repeat the entire set of steps.	Recommend changing the text to "The attended authentication of PIV Biometric is nearly the same as unattended authentication, except that the attendant observes submission of the biometric sample, thus increasing protection against spoofing."	Resolved by removing the steps 1-9 (lines 1735-1749) and modifying the sentence as follows. "This authentication mechanism is the same as the unattended biometrics (BIO) authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder."
DoD-63	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	56	1760	6.2.4.1	The "Authentication with the PIV authentication certificate credential (PKI-AUTH)" section only mentions the use of a PIN to activate the card. How will this section allow for other activation mechanisms that are expected to be specified in [SP 800-73]?	Recommend including a hook to reference other activation mechanisms (e.g., On-Card Biometric Comparison) as specified in [SP 800-73].	Resolved by the following changes: - Combine steps 2 and 3. - Add a sentence – If implemented, other card activation mechanisms, as specified in [SP 800-73], may be used to activate the card. - Change the characteristics to - Strong resistance to use of unaltered card by non-owner since card activation is required.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-64	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Technical)	57	1811	6.2.6	Document says, "The card responds to the previously issued challenge by signing it using the symmetric card authentication key." Symmetric keys are not capable of signature.	Recommend changing the text to "The card responds to the previously issued challenge by encrypting the challenge using the symmetric card authentication key."	Accept.
DoD-65	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(General)	58	1820-1823	6	The statement "Two or more complementing identity authentication mechanism may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder. For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in cardholder identity." is somewhat misleading, when considered in the context of OMB-04-04 E-Authentication Levels described earlier in the section. If PKI-AUTH already provides "VERY HIGH Confidence" for Physical and Logical (both Local and Remote) Access by itself, what sort of credit is given towards the additional application of BIO (i.e., what is the incentive to perform the extra step)? Requires clarification.	Recommend clarify the reason or incentive to perform the extra BIO step, given that PKI-AUTH provides "VERY HIGH Confidence".	Declined. We would like to maintain consistency with SP 800-63, which requires two factors of authentication for VERY HIGH assurance level. We note that Table 6-2 defines the minimum requirement for each assurance level. FIPS 201-2 Section 6.3, introductory paragraph already says "Two or more complementing authentication mechanisms may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder. For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in cardholder identity."
DoD-66	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Editorial)	61	1915	A.4	There may be some confusion with the phrase, "...validated to FIPS 140 with an overall Security Level 2 (or higher). [FIPS140-2]" Some may think the "-2" is the level.	Recommend changing the text to "...validated to [FIPS 140-2] or later certified to an overall security level of 2 (or higher). "	Resolved by ICAMSC-161.
DoD-67	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	Substantive (Technical)	62	1934-1946	Appendix B	Appendix B: Description of the NACI: Recommends this detail be removed. The NACI will be replaced by Tier 1 when the new Federal Investigative Standards are promulgated.	Recommend changing the text to "NACI or equivalent investigation as determined by Federal Investigative Standards" and leave out details.	Resolved by OPM-6.
DoD-68	DoD	Jonathan Shu, 831.583. 2400, jonathan. shu@osd .mil	(Editorial)	64	1955	D.1	Missing useful information.	Recommend expanding the table to include the Policy OIDs as well so that all OIDs could be found in one location.	Resolved by ICAMSC-164.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DoD-69	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Editorial)	71	2171	E.2	Several acronyms are used within the document but are not included in this appendix.	Recommend adding the following acronyms to appendix E: AID, CST, CV, FSM, OCC, OCONUS, OGP, PIA, PII, and SSP.	Resolved by adding AID, OCC, PII, and SSP to list of acronyms and by removing all uses of the acronyms CST, CV, FSM, OCONUS, and OGP.
DoD-70	DoD	Jonathan Shu, 831.583.2400, jonathan.shu@osd.mil	(Editorial)	74	2267	F	Several documents used in the text of this document are not referenced.	Recommend adding the following references: FISMA 2002, 44 U.S.C., and the Internal Revenue Service Manual.	Resolved by adding reference to FISMA 2002 and SP 800-59 (Guideline for Identifying an Information System as a National Security System), and by including URL for Internal Revenue Service Manual in the footnote that references the manual.
DOE-53	ICAMSC	Glen Lee (DOE OCIO)	T	10	545-546	2.5.2	"The PIV Card itself is revoked. Any local databases that contain FASC-N values must be updated to reflect the change in status." Revocation of a PIV Card is directly tied to the revocation of the PIV Auth Cert. There is no other interoperable means of revoking and/or checking the revocation status of a PIV Card.	Recommend deleting the quoted statements. As written, updating databases containing FASC-N is a requirement that willl never be met. The requirement is correctly stated in lines 547-556. All relying party systems are obligated to check the CRL/OCSP responders.	Resolved by Cert-34.
DOE-54	ICAMSC	Glen Lee (DOE OCIO)	T	10	547	2.5.2	The statement implies that all certificates must be revoked, even those that have not been compromised or have the potential for being compromised. Revoking all certiicates all the time will make CRLs unneccessarily large. if there is a potential for compromise of the key the certificate needs to be revoked. Common Policy CP has specific procedures on revocation.	Replace current text about revocation request procedures with a reference to Common Policy CP.	Resolved by DHS-5.
DOE-89	ICAMSC	Glen Lee (DOE OCIO)	T	38	1177	4.2	The statement that a CHUID should be treated as if it were a password doesn't make sense. A CHUID is an identifier and can be obtained from anyone with a contactless reader and proximity to the card. A password is typically used in conjunction with an identifier and is kept secret. Although it is not considered the greatest security, passwords are far more secure than a CHUID used by itself for access.	Recommend replace the current text with the following: The CHUID may be read and used by the relying systems as an identifier only for the purposes of authentication . The CHUID is not resistent to cloning; therefore it may be copied and used to gain access to systems that solely rely on the presentation of a CHUID.	Resolved by removing the third paragraph of Section 4.2 (new Section 4.2.1), lines 1184-1187. Decline to indicate that PII data should be encrypted since it is already covered by FISMA.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOE-135	ICAMSC	Glen Lee (DOE OCIO)	G	49	1566	5.5	"CAs that issue authentication certificates shall maintain an LDAP directory server that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it." The text, as is, implies that HTTP is optional for CRL Distribution Points (CDPs) of certificates on the PIV Card. HTTP should also be called out as a mandatory source for CRLs. Moreover, the text reinforces the continued use of of LDAP for CDPs, which agencies are blocking at the firewalls. FIPS 201 should indicate LDAP is deprecated.	Recommend replacing the current text with the following: "As that issue authentication certificates shall maintain a repository that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it. The repository shall make CRLs available via HTTP 1.1. LDAP is deprecated."	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2. Section 5.5.1 (Line 1573) of the first public-comment draft of FIPS 201-2 states that distribution of CRLs using HTTP is required, and we do not intend to remove that requirement. The above mentioned documents also require distribution of CRLs using HTTP and require certificates to include HTTP URIs in cRLDistributionPoints extensions.
DOE-138	ICAMSC	Glen Lee (DOE OCIO)	T	49	1573	5.5.1	The document says, "This standard requires distribution of CA certificates and CRLs using LDAP and Hypertext Transport Protocol (HTTP)." LDAP should be deprecated.	Recommend changing text to "This standard requires distribution of CA certificates and CRLs using Hypertext Transport Protocol (HTTP). LDAP is deprecated."	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.
DOE-139	ICAMSC	Glen Lee (DOE OCIO)	G	50	1576 - 1581	5.5.1	This section appears to suggest that any x.509 certificate that contains the FASCN or some representation of the FASCN cannot be make publically available. Intrinsically, public certificates are made available to the public to support the verification of digital signatures. Without understanding the security concerns/risks of the FASCN within a public certificate, it doesn't make sense for FIPS 201 to require the limited distribution of a certificate. Especially, when the CHUID, which contains the FASCN, is a free read on contact and contactless interfaces of the PIV.	Strongly recommend deleting this requirement. It suggests the FASCN is a secret instead of an identifier.	Resolved by DoD-61.
DOJ-1	DOJ	Eric Olsson	G	2	250	1.3	All the changes proposed in this Draft will be difficult to implement all at one time across an entire agency or shared service and no information on adoption or migration is provided. For example it will take many months to be ready at all locations to handle a second 1:1 biometric match of iris images.	Add a subsection to Change Management or another section that describes in more detail the expectations for transitioning from FIPS 201-1 and implementing the changes included in FIPS 201-2 before this draft version is finalized.	Declined. Resolved by DoD-3.
DOJ-2	DOJ	Eric Olsson	T	6	394	2.3	Identity proofing source documents change or may need further clarification over the next 5-year period.	Remove the list of approved documents from FIPS 201-2 and include a reference to a Special Publication for the approved ID source documents.	Resolved by ICAMSC-23.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOJ-3	DOJ	Eric Olsson	T	8	465	2.4	The sixth bullet requires a 1:1 biometric match of the applicant against the biometric included in the PIV Card. A small percentage of existing cards can't be successfully matched using a biometric on the card.	Allow any existing PIV Cards to be issued without a 1:1 biometric match of the fingerprints or iris images at the time FIPS 201-2 takes effect until all existing cards are activated. Allow an Activator to match the applicant to the card using the picture on the card along with a primary ID from Section 2.3.	Accept to address failed biometric match per the new text introduced by DOT-11.
DOJ-4	DOJ	Eric Olsson	T	9	508	2.5.1	The second line of this paragraph states, "The original PIV Card must be surrendered when requesting a renewal."	The PIV Card should be surrendered when activating the new PIV Card during the renewal process.	Resolved by deleting the sentence and revising the sentence: "The original PIV Card must be collected and destroyed" to "Prior to receiving the new PIV Card, the cardholder shall surrender the original PIV Card, which shall be collected and destroyed when the new PIV Card is issued."
DOJ-5	DOJ	Eric Olsson	T	9	517	2.5.1	The renewal process allows a 12 week timeframe for renewal of PIV Cards. FIPS should allow for special circumstances where a PIV Card needs to be renewed more than 12 weeks prior to expiration (e.g., when staff are being deployed overseas.)	Allow PIV Cards to be renewed up to one year prior to expiration.	Resolved by DHS-4.
DOJ-6	DOJ	Eric Olsson	T	9	518-519	2.5.1	In the second paragraph, second line it states, "The cardholder will not be allowed to start the renewal process if the original PIV Card is expired." It is not clear when the renewal process "starts".	Clarify when the renewal process starts (i.e., when the Sponsor applies for the cardholders card be renewed, when the cardholder attempts to activate the new card, or other.) Allow the cardholder to activate a new card as part of the renewal process within 30 days of the original PIV Card expiration as long as the new card renewal process was initiated by the Sponsor prior to the original card expiration.	Resolved by the following: Change line 509 to, "The renewal process for a PIV Card starts when a proper authority authorizes the renewal of the credential." Also, add the following sentence to the first paragraph: "The entire identity proofing, registration, and issuance process, as described in Sections 2.7 and 2.8, shall be repeated if the issuer does not maintain a chain-of-trust record for the cardholder or if the renewal process was not started before the original PIV Card expired."
DOJ-7	DOJ	Eric Olsson	T	11	596	2.5.4	The last bullet in this section states, "If the PIV Card post issuance update begins but fails for any reason, the PIV Card issuer shall immediately terminate the PIV Card as described in Section 2.5.6, and a diligent attempt shall be made to collect and destroy the PIV Card." Post issuance updates may fail and then be recoverable by the PIV Card issuer during the same visit by the PIV Card holder to a remote station. PIV Cards recovered and corrected to the appropriate state should not need to be destroyed or replaced. Currently, this occurs frequently using the GSA Shared Service and would be an expensive and time consuming burden on the agency to replace all PIV Cards that fail during the post issuance update process.	The last bullet should be removed from the standard. Details of the type of error, the ability to recover from the error, and update process should be left up to the issuer.	Resolved by DoD-27.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOJ-8	DOJ	Eric Olsson	T	15	710	3.1	The Functional Components section 3.1 is out of sync with the FICAM guidance.	Bring this section and definitions into compliance with the latest FICAM Segment Architecture and the FICAM Roadmap.	Resolved by Cert-47.
DOJ-9	DOJ	Eric Olsson	T	23	943	4.1.4.1	The second paragraph of this section states "Zone 2F—Name. The full name shall be printed directly under the photograph in capital letters." This statement conflicts with lines 954 and 955 where names other than the first and last name may be abbreviated.	Make it clear that the middle name may be abbreviated on the card.	Move lines 954-960 to above the table and below line 951. Also, insert a new row after 2nd row and provide an example of abbreviated middle name as follows: Anna Maria Eriksson - Eriksson, Anna M.
DOJ-10	DOJ	Eric Olsson	T	36	1132	4.1.6.1	The fourth bullet states, "Two biometric fingerprints or if fingerprints are not collectible, two iris images". The requirement for 2 iris images conflicts with other sections of the Draft where 1 or 2 iris images shall be collected as option data elements.	Remove the requirement here to capture 2 iris images.	Replace "Two biometric fingerprints or if fingerprints are not collectible, two iris images" with "two fingerprint templates"
DOJ-11	DOJ	Eric Olsson	T	38	1184 - 1187	4.2	This section states the CHUID should be treated as a password. The CHUID is less significant than a password.	Remove the requirement here to store the CHUID as a password.	Resolved by Cert-73.
DOJ-12	DOJ	Eric Olsson	T	42	1340 - 1342	4.4.1	The second sentence of this section states, "The chain-of-trust is a sequence of related enrollment data records, and shall be created and maintained through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records." And footnote 11 states, "For example, ten fingerprints for law enforcement checks may be collected at one time and place, and two fingerprints for PIV Card templates may be collected at a later time and different place, provided that the two fingerprints are verified as among the ten original fingerprints. The DOJ requires that the either the NACI, NACI waiver, or higher security clearance be approved before an employee or contractor begins work with the DOJ. DOJ collects fingerprints for submittal to the FBI NCHC using various methods including electronic scanning using the Civil Applicant System (CAS) and via fingerprint cards at police stations around the country. The CAS system is not integrated to the GSA's USAccess system used by DOJ for PIV Card enrollments and activations. Current PIV Card holders at DOJ and across most of the other Federal agencies do not have fingerprints that were captured at enrollment that have been electronically submitted to the FBI NCHC. Making this a requirement for all PIV Card holders will be cost prohibitive.	Recommend removing footnote 11 and allowing the chain of trust to be initiated during the PIV Card enrollment process without re-checking the fingerprints collected at enrollment with the FBI fingerprint database.	Declined. Resolved by WM-24. Note: The collection of the 10 prints is not required if a favorably adjudicated NACI / background investigation has been located.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOJ-13	DOJ	Eric Olsson	T	43	1370	4.4.1	The second sentence of this paragraph states, "The fingerprints shall be used for one-to-many matching with the database of fingerprints maintained by the FBI." The DOJ collects fingerprints for submittal to the FBI NCHC using various methods for the BI and NACI process. Once the waiver or NACI is approved, the applicant then proceeds to enrollment where 2 IDs are proofed and 10 fingerprints are captured for the PIV Card chain of trust. Using the PIV Card enrollment process to collect 10 fingerprints for the FBI NCHC would be cost prohibitive when initiating BI for staff in remote areas or for staff in positions with high NCHC failure rates such as prison guards.	Recommend removing the statement "The fingerprints shall be used for one-to-many matching with the database of fingerprints maintained by the FBI." from section 4.4.1, or make it clear that these are not required to be the fingerprints collected at enrollment. See also comment 12.	Resolved by DOJ-12, paragraph 2.
DOS-1	DOS	MSulak	G	VI	169	9	This section states that the standard is Effective Immediately yet says that the requirements are in accordance with OMB timetable. This needs to be clarified.	Remove the sentence "This standard is effective immediately."	Resolved by DoD-3.
DOS-2	DOS	MSulak	E	6	406	2.3	A drivers licenses is an ID issued by a Federal, State or Local entity therefore it should be removed or swapped/combined with line 417 page 7.	Combine lines 406 and 417 into the primary ID source.	Declined. There are some ID source documents that are covered by line 417 that are inappropriate as primary source documents.
DOS-3	DOS	MSulak	E	6	410	2.3	A DOD CAC IS a federal issued identity card and does not need to be listed separately.	Remove line 410, page 6.	Declined. The PIV Card, which includes CAC, counts as a primary source document. Other unspecified federal identity source documents are secondary documents.
DOS-4	DOS	MSulak	E	26	1023	4.1.4.3	The location of Zone 18F is not depicted on any of the card layouts	Place a Zone 18F identity marker on figure 4.3 to locate the area of discussion.	Resolved by adding a label to Zone 18F in Figure 4-1.
DOS-5	DOS	MSulak	E	26	1023	4.1.4.3	The discription of Zone 18F can be confusing and misleading as written.	Move the last sentence in the Zone 18F discription to the first sentence position. It shold now read: If Zone 16F photo border coloring is used to identify employee affiliation of emergency response officials, foreign nationals, or contractors, the lettering shall correspond to the printed color. The affiliation color code "B" for Blue, "G" for Green, or "R" for Red shall be printed in a white circle in Zone 15F. The diameter of the circle shall not be more than 5 mm. Note that the lettering shall correspond to the printed color in Zone 15F.	Resolved by removing reference to Zone 16F.
DOS-6	DOS	MSulak	E	46	1479	4.5.2	The section talks about Contactless Readers yet the third sectence states Contact Readers. It reads: Specifically, the contact card readers shall conform to the requirements specified in [SP 800-96]	Change the wording to Contactless	Resolved by AMAG-10.
DOS-7	DOS	MSulak	E	64	1952	D.1	This section is more technical, not meant for the FIPS, therefore it shoud be moved to a Special Publication.	Transfer this section to SP 800-73-3.	Declined. The appendix provides a convenient reference for FIPS 201 identifiers.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOS-8	DOS	MSulak	E	66	1986	E.1	The glossary does not define what a CHUID, GUID or a UUID is as discussed in the FIPS.	Add a definition for the CHUID, GUID and UUID.	Declined.
DOS-9	DOS	MSulak	E	71	2172	E.2	There is no acronym listed for the GUID or UUID.	Add the acronym for the GUID and UUID.	Accept.
DOT-1	U.S. DOT	Martha Pogue	E	v	135	6. Applicability	OCONUS is being used for the only time in the draft and it's not defined. Suggest rewording.	Suggest changing, "with particularly sensitive OCONUS threats" to "with particularly sensitive threats from outside the contiguous United States."	Accept.
DOT-2	U.S. DOT	Martha Pogue	G	v	154	8. Implementations	HSPD-12 does not specify that the credential has to be in the form of a card. With the growing mobile workforce, there is a need to support other form factors.	Suggest allowing alternative form factors as long as they can be tied to the Chain-of-Trust record.	Resolved by introducing the concept of derived credentials and providing a reference to Special Publication 800-157.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOT-3	U.S. DOT	Martha Pogue	G	vi	194	11. Waiver s	This sentence indicates that waivers to Federal Information Processing Standards are not allowed. In reviewing the Federal Information Security Management Act of 2002, nothing is mentioned as to waivers except that these standards are mandatory in reference to § 11331(b). Is this the language where the "no waiver" conclusion is being derived? The Act also states that the President may disapprove or modify Federal Information Standards and Guidelines if such action is in the public interest. (See § 11331(c))		The following explanation appears in Section 3.2 of the FAQ for the Cryptographic Module Validation Program: With the passage of the Federal Information Security Management Act (FISMA) of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards (FIPS). The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supercedes that Act. Therefore, the references to the "waiver process" contained in many of the FIPS are no longer operative. FIPS do not apply to national security systems (as defined in FISMA). Additional detail: The Computer Security Act of 1987 (Public Law 100-235) established a statutory basis for the waiver of Federal Information Processing Standards, or FIPS. Section 4 of the Act amended section 111(d) of the Federal Property and Administrative Services Act of 1949. As part of this amendment 40 USC 759(d)(3) authorized the Secretary of Commerce to waive FIPS under certain conditions. Section 5131 of the Information Technology Management Reform Act (Clinger-Cohen) (Public Law 104-106) repealed 40 USC 759(d), but reenacted it in substantially identical form as 40 USC 1441. The waiver authority continued as before, as section 5131(c) of the Act, or 40 USC 1441(c). On August 21, 2002 the President signed Public Law 102-217, which substantially revised title 40 of the United States Code. Section 5131 of Clinger-Cohen was repealed but reenacted as section 11331 of title 40. Section 11331(d) continued the FIPS waiver provisions as they had been previously. Title X of the Homeland Security Act of 2002 (Public Law 107-296) contained the first Federal Information Security Management Act of 2002 (FISMA), and was signed into law on November 25, 2002. Section 11331 of title 40 of the United States Code was substantially amended by FISMA, and the authority to waive FIPS was repealed and not reinstated. Title III of the E-Government Act contains the second Federal Information Security Management Act of 2002 (Public Law 107-347), signed into law on December 17, 2002. Section 11331 of title 40 of the United States Code was again substantially amended, but the authority to waive FIPS repealed by the Homeland Security Act was not reinstated. Hence, no authority exists under current law to waive FIPS.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOT-4	U.S. DOT	Martha Pogue	E	1	231	1.2	Since we're in a new administration, suggest specifying which President signed HPSD-12.	change "signed by the President" to "signed by President George W. Bush"	Accept.
DOT-5	U.S. DOT	Martha Pogue	E	2	251	1.3	"new revision" is redundant	strike "new"	Accept.
DOT-6	U.S. DOT	Martha Pogue	G	vi	169 - 171	9. Effective Date	Most of these changes will require lead time to implement, especially those for which there are no solutions in the marketplace yet.		Noted.
DOT-7	U.S. DOT	Martha Pogue	T	5	360	2.1	A credential is issued only after NACI or equivalent is initiated **and the FBI NCHC is completed.** This wording implies the NCHC must be conducted as a separate check from the NACI.	A credential is issued only after NACI or equivalent is initiated and **at a minimum** the FBI NCHC is completed.	Resolved as per discussion with OPM and OMB. Resolved by replacing the 2nd bullet with the following: + A credential is issued only after National Agency Check with Written Inquiries (NACI) (or equivalent or higher) or Tier 1 or higher federal background investigation is initiated and the FBI National Criminal History Check (NCHC) portion of the background investigation is completed.
DOT-8	U.S. DOT	Martha Pogue	T	6	388	2.3	Are there other biometric identifiers permitted? What about individuals with targeted disabilities who may not have hands/fingers?	There needs to be the ability to provide either an alternative biometric or a completely different non-biometric alternative for people who cannot provide either fingerprints or iris images due to temporary or permanent disability.	Resolved by text in Section 4.4.1 (now Section 2.3) line numbers 1374-1377, that advises agencies to seek OPM guidance. Note: idmanagement.gov has addressed alternatives. See answer to question 2 at http://www.idmanagement.gov/documents/hspd12_faqs_biometric.pdf: "For the purposes of the criminal history check, there is no alternate biometric. Where prints are not available, OPM will rely on the name check for criminal history."
DOT-9	U.S. DOT	Martha Pogue	T	6	391	2.3	Suggest adding language that if the applicant is a foreign national, one of the identifying documents must provide legal status so this can be established early in the process and time isn't wasted and agencies are in compliance with ICE. Leaving the choice of documentation to the FN doesn't establish their legal status. This requires more time and effort at the back end when they have already entered our facilities to initiate this process.	Suggest adding language that if the applicant is a foreign national, one of the identifying documents **must** be legal status (Form I-551 or Form I-766)	Resolved by adding a footnote at the end of the following sentence: "During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form." that says: "Departments and agencies may choose to accept only a subject of the identity source documents listed in this section. For example, in cases where identity proofing for PIV Card issuance is performed prior to verification of employment authorization, departments and agencies may choose to require the applicant to provide identify source documents that satisfy the requirements of Form I-9, Employment Eligibility Verification, in addition to the requirements specified in this section. "
DOT-10	U.S. DOT	Martha Pogue	T	6	409 - 410	2.3	Individuals changing jobs, either within or between deparmtments or agencies, may already have a PIV card.	Change, "...ID card; or" to "...ID card;" Change "… Access Card." to "… Access Card; or" and insert new line, new bullet, "- PIV Card."	Resolved by replacing the Common Access Card with the PIV Card on the list. Note: The chain-of-trust mechanism may be used to eliminate the need to repeat the complete registration and issuance process in these cases.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOT-11	U.S. DOT	Martha Pogue	T	8	465 - 469	2.4	There is a problem for individuals with multiple disabilities, i.e., no hands/fingers and also unable to allow a successful iris scan. There need to be alternatives for these people who, through temporary or permanent disability, cannot provide these biometrics.	There needs to be the ability to provide either an alternative biometric or a completely different non-biometric alternative for people who cannot provide either fingerprints or iris images due to temporary or permanent disability.	Replace Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the applicant against the biometric included in the PIV Card. The 1:1 biometric match requires either a match of fingerprint(s) or a match of iris image(s). Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. On successful match, the PIV Card shall be released to the applicant. with Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the applicant against biometrics available on the PIV Card. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. On successful match, the PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide two identity source documents (as specified in Section 2.7), and a attending operator shall inspect these and compare the cardholder with the facial image printed on the PIV Card.
DOT-12	U.S. DOT	Martha Pogue	G	8	472	2.4	With normal physical access usage agencies currently report that PIV cards now typically last about 18 months before they begin to deteriorate. With increased card use for logical access in the future we expect this 18 month period to shorten. This proposal extends the validity of PIV cards from 5 years to a longer period of 6 years. Since the cards are not now durable enough to withstand 5 years of usage we do not understand how they will possibly last for 6 years.		The six year timeline has been requested by agencies to synchronize with certificate expiration.
DOT-13	U.S. DOT	Martha Pogue	T	8	473 - 475	2.4	The term "PIV Issued Cards" is not in the definitions. If the idea is that these cards are not valid or are not vailid for issuance then say that. Suggest rewording.	Change to, "Cards that contain topographical defects (e.g. scratches, poor color, fading, etc.), contain errors in optional fields, are not properly printed, or are not delivered to the cardholder are not considered to be PIV Cards."	Resolved by Cert-18.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOT-14	U.S. DOT	Martha Pogue	T	9	486 - 489	2.4.1	The pseudonym should be tied to the identity of the individual, presumably in the identity management system, as long as the adequate protections are in place to protect even the existance of the pseudonym from unauthorized personnel. Also, the process of issuing PIV Cards with pseudonyms should be different and distinct from that of a legal name change as the employee may need to keep a PIV Card with his or her legal name.	Suggest writing a separate section on the issuance of pseudonymous cards.	Declined. A separate section on issuance of pseudonymous cards is not necessary since the process is not different from issuance of other cards, except (and as pointed out) that the pseudonym is stored in the enrollment record. Protection of data is subject to FISMA. Resolved by Cert-19.
DOT-15	U.S. DOT	Martha Pogue	T	9	506 - 575	2.5.1 & 2.5.2	There still is not a clear distinction between "renewal" and "reissuance" and what the requirements are that drive towards one versus the other. Suggest adding text to clearly state intent. The intent of renewal is to replace a current PIV Card that is about to expire with a PIV Card with new PIV Card with a later expiration date. The intent of reissuance is to replace a current PIV Card that has been damaged, lost, stolen, or compromised with a new PIV Card that has an expiration date which is the same or later than that of the current PIV Card.	See attached re-write	Resolved by new text.
DOT-16	U.S. DOT	Martha Pogue	T	9	508 - 509	2.5.1	The PIV Card must be surrendered before the recipient may receive a replacement card but should not have to be surrendered before the new PIV card is issued. Also, the word "original" makes sense when the employee has received only one PIV card, but if the employee has replaced the card for any reason the word "original" doesn't apply.	Change, "The original PIV Card must be surrendered when requesting a renewal." to "The current PIV Card must be surrendered before the recipient may be issued a replacement PIV Card."	Resolved by DOJ-4.
DOT-17	U.S. DOT	Martha Pogue	G	9	510	2.5.1	What if the issuer is someone who does not have access to eOPF nor is trained to userstand what constitutes an up to date personnel record? What constitutes "in good standing?"	The person who authorizes the renewal of the PIV Card should be the one to verify the employee is in good standing. Also suggest adding definition for "in good standing."	Resolved by replacing "The issuer shall verify that the employee remains in good standing and personnel records are current before renewing the card and associated credentials. When renewing identity credentials for current employees, the NACI check shall be followed in accordance with OPM guidance " with: "The issuer shall verify that the employee's or contractor's background investigation is valid before renewing the card and associated credentials. Re-investigations shall be performed if required, in accordance with OPM guidance." as discussed with OPM/OMB.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOT-18	U.S. DOT	Martha Pogue	T	9	514	2.5.1	What if neither biometric is available? Are there other options?	See comment #8. Is providing a primary identity source document per Section 2.3 acceptable?	Replace (lines 513-514): The issuer shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or a match of iris image(s). Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. with: The issuer shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. On successful match, the new PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide the original PIV Card and another primary identity source document (as specified in Section 2.7), and an attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment record and the facial image printed on the new PIV Card.
DOT-19	U.S. DOT	Martha Pogue	E	13	643	2.5.6	The acronym IIF is used for the first time and hasn't been defined.	Change to, "The Information in Identifiable Form (IIF) is used…"	Declined. All instances of IIF will be replaced by PII, and a reference to the OMB definition will be provided.
DOT-20	U.S. DOT	Martha Pogue	T	14	696	2.7 (new)	This might be a good place to state the Accessibility Requirements, pursuant to Sections 501, 504, and 508 of the Rehabilitation Act of 1973, as amended.	Add statements reiterating that pursuant to Sections 501, 504, and 508 of the Rehabilitation Act of 1973, as amended, and that PIV programs must be implemented in such as way as to not create additional barriers for Federal and contractor employees with disabilities and which would clearly state the government's intent to provide reasonable accomodation for individuals with disabilities and also to summarize in one place the different types of accomodations that may be made.	Text has been added to Section 8 of the Announcement (Implementations) reminding agencies of their responsibilities under Sections 501, 504, and 508 of the Rehabilitation Act of 1973.
DOT-21	U.S. DOT	Martha Pogue	T	15	712 - 714	3.1	HSPD-12 does not specify that the credential has to be in the form of a card. With the growing mobile workforce, there is a need to support other form factors.	Suggest allowing alternative form factors as long as they can be tied to the Chain-of-Trust record.	Resolved by creating a new special publication that will address derived credentials for other form factors such as mobile phones and tablets. The card form factor for PIV Card continues to remain the primary PIV credential for security and interoperability purposes.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOT-22	U.S. DOT	Martha Pogue	T	21	893	4.1.3	The first sentence reads, "Departments and agencies shall ensure that the card meets the requirements of Section 508 of the Rehabilitation Act." Do you mean Section 504 as opposed to 508 since 508 deals with electronic information technology and Section 504 deals with access to Federally conducted programs and activities? The example given is raised Braille on the card which is a physical characteristic. The application itself would need to be Section 508 compliant so I'm not sure how the card alone would deal with Section 508 requirements, unless it would be referring to the technical standards for self-contained, closed products pursuant to 36 CFR 1194.25(d). Additionally, Section 501 covers reasonable accommodation in employment situations if an employee needed an accommodation in order to use the card, e.g., someone putting the card into a computer for the employee. Perhaps this sentence could be further clarified.	Please clarify these sections.	Resolved by new text.
DOT-23	U.S. DOT	Martha Pogue	T	36	1132	4.1.6.1	Are there other biometric identifiers permitted? What about individuals with targeted disabilities who may not have hands/fingers?	There needs to be the ability to provide either an alternative biometric or a completely different non-biometric alternative for people who cannot provide either fingerprints or iris images due to temporary or permanent disability.	Accept in principle - FIPS 201 requires storage of facial image and allows, but does not require, storage of iris. See also DOT-18.
DOT-24	U.S. DOT	Martha Pogue	T	42	1317	4.4	The use of "shall" implies that the following list of items is mandatory. Currently, the Department is able to decide when there can be accommodations made for individuals who cannot be fingerprinted. Similar flexibility should be encouraged here as well.	Change to, " The PIV biometric data shall consist of the following, except where fingerprints are unable to be collected due to temporary or permanent disability."	See NCE-37.
DOT-25	U.S. DOT	Martha Pogue	T	42	1319	4.4	What if a full set of fingerprints is not available, e.g., a person without fingers/hands?		Resolved by text in Section 4.4.1 (now Section 2.3) line numbers 1374-1377, that advises agencies to seek OPM guidance. Note: idmanagement.gov has addressed alternatives. See answer to question 2 at http://www.idmanagement.gov/documents/hspd12_faqs_biometric.pdf: "For the purposes of the criminal history check, there is no alternate biometric. Where prints are not available, OPM will rely on the name check for criminal history."
DOT-26	U.S. DOT	Martha Pogue	T	42	1320 - 1321	4.4	Has facial imaging gotten good enough to be used as an alternative biometric for individuals for whom fingerprints or iris images cannot be collected due to a temporary or permanent disability?	Suggest that facial biometric stored on card may be acceptable alternative biometric for individuals for whom fingerprints or iris images cannot be collected due to temporary or permanent disability.	Noted. FIPS 201 will allow agencies to use automated facial comparison for attended processes. This is supported by the existing standardized facial image specifications.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOT-27	U.S. DOT	Martha Pogue	T	44	1393	4.4.2	If the facial biometric is adequate to authenticate cardholders for whom fingerprints or iris images cannot be collected, why does it seem to appear here as an afterthought instead of being mentioned throughout the standard such as iris images are?	suggest recommending the use of facial biometrics throughout the standard, much like iris images, as an alternative to fingerprints for individuals for whom fingerprints cannot be collected. In cases where biometrics that are less than 12 years old may be reused, maybe 5 or 6 years is better in the case of facial biometrics.	Noted. See DoD-51, agencies are free to implement automated iris or automated face in cases where fingerprints are not usable. Manual visual comparison has been reported inferior to automated face, fingerprint, and iris recognition.
DOT-28	U.S. DOT	Martha Pogue	T	44	1413	4.4.2	How will keys for asymmetric cryptography be released to persons requiring this method? Will there be a standardized, secure method?		The PIV Authentication key is already mandatory for all cards.
DOT-29	U.S. DOT	Martha Pogue	T	56	1762 - 1764	6.2.4.1	As PKI-AUTH is designated the standard for persons who cannot have fingerprint/iris images, it may also be important for the asymmetric cryptography key to change, much like a password, in order to comply with OMB’s E-Authentication Level 4. The issue of persons lacking the dexterity to manipulate the card properly is still a concern. In addition, PKI-AUTH requires a PIN number and response. Will a person be able to use an audio format to respond to PKI-AUTH requirements? Will a PKI-AUTH-A standard, in addition to a BIO-A standard, also be considered?		The technical requirements for satisfying E-Authentication Level 4 are specified in NIST Special Publication 800-63-1, which specifies in Appendix B that the certificate policy Common-Auth satisfies E-Authentication Level 4. PIV Authentication certificates are issued under the Common-Auth certificate policy, and thus the PKI-AUTH authentication mechanism does satisfy E-Authentication Level 4. The Common-Auth certificate policy currently limits the lifetime of an authentication key to 3 years. FIPS 201 specifies authentication mechanisms that are supported by PIV Cards, but departments and agencies are responsible for the designs of the physical and logical access control systems, including the selection of appropriate authentication mechanisms and ensuring that requirement for accessibility are satisfied. BIO-A is listed as a separate authentication mechanism from BIO, since the presence of an attendant who can guard against attempts to use fake biometrics (e.g., a gummy finger) increases the level of assurance of the authentication mechanism. There is no corresponding benefit to the use of an attendant with the PKI-AUTH authentication mechanism, and so there are no plans to consider the addition of a PKI-AUTH-A authentication mechanism. PKI-AUTH does not preclude an assistant from helping a cardholder with authentication.
DOT-30	U.S. DOT	Martha Pogue	E	57	1800	6.2.5		After the word “biometric” please delete the small a and capital I and replace as follows: “biometric, if agencies choose…”	Accept.
DOT-31	U.S. DOT	Martha Pogue	E	57	1800	6.2.5		After the word “implement” change the capital O in “On-card” to “on-card.”	Accept.
DOT-32	U.S. DOT	Martha Pogue	T	59	1855	Table 63	PKI-AUTH+PIN should be included in HIGH confidence for authentication to local workstations.	Include PKI-AUTH+PIN as an option to BIO for HIGH confidence to local workstation environments	Declined. PKI-AUTH is already ranked VERY HIGH and FIPS 201 already states: An authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
DOT-33	U.S. DOT	Martha Pogue	T	59	1855	6.3.2	For remote access using PKI-AUTH or PKI-CAK, are alternate form factors of the PIV card/PIN entry built into the system? Many people may not have the manual dexterity to use the normal card as it stands, and at home for remote access, could face more issues.		Declined. There are system implementations that enhance PIV Card usage to address specific user needs. Defining such system behavior is outside the scope of FIPS 201.
DOT-34	U.S. DOT	Martha Pogue	E	61	1893	A.2		Delete "in" before "pursuant"	Accept.
DOT-35	U.S. DOT	Martha Pogue	E	63	1949	C		Add “ed” at the end of “intend.”	Resolved by deleting Appendix C.
DOT-36	U.S. DOT	Martha Pogue	T	66	2014 - 2015	E.1	Add "Backend Attribute Exchange" and define it.	Backend Attribute Exchange: Standard mechanism for Relying Parties to obtain PIV Cardholder information (Backend Attributes) from the Authoritative Source (Attribute Authority).	Resolved by Cert-21. Backend Attribute Exchange is removed from the document and therefore its definition is not necessary.
DOT-37	U.S. DOT	Martha Pogue	E	71	2180	E.2	Among the list of acronyms, this line is the only one in bold. Is there a reason for this?	Remove the bolding	Accept.
DOT-38	U.S. DOT	Martha Pogue			12713		This is a comment on the Federal Register Noticeand Request for Comments for the Draft FIPS 201-2: Section 508 of the Rehabilitation Act, and not Section 508 of the Americans with Disabilities Act, is the applicable statute covering electronic and information technology accessibility for individuals with disabilities.	Revise, “Section 4.1.4.3 is added to provide requirements for compliance with Section 508 of the Americans with Disabilities Act,” to “Section 4.1.4.3 is added to provide requirements for compliance with Section 508 of the Rehabilitation Act of 1973, as amended.”	Noted.
DSS-1	Document Security Systems	David Wicker	G				A comment on security features for the PIV card that pertains to section 4.1.2 of the FIPS 201-2 draft document. We have developed a "watermark" internal to the card substrate that is currently being utilized for drivers license verification.		Noted. Agencies might elect to adopt techniques like this.
ES-1	Electrosoft Services Inc.	Sarbari Gupta	G	6	169	9	"This standard is effective immediately". Certain sections of this revision cannot be implemented until the final release of other specifications which will not be published immediately, such as an update to SP 800-73 along with SP 800-85A/B and the associated tools.	Change to: "This standard is effective immediately; those sections of this standard that depend upon the release of other specifications and/or revised Special Publications are effective immediately upon final publication of the dependent specifications."	Resolved by DoD-3.
ES-2	Electrosoft Services Inc.	Sarbari Gupta	G	1-2	259-283	1.3.1-1.3.4	Change management information is extremely useful to identify areas of change. Use of 'For example' to identify changes for a revision is non-specific to a FIPS 201 release and is subject to mis-interpretation.	Change 'For Example' to "Changes in this revision include:' and then list each major change in the revision as a bullet item.	Declined. Section 1.3 provides guidelines and principles for the Change Management. An informative revision history is provided in Appendix E.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ES-3	Electrosoft Services Inc.	Sarbari Gupta	E	8	472	2.4	"The PIV Card shall be valid for no more than six years." The current GSA FIPS 201 EP durability testing criteria for PIV Cards uses, as one of its bases, the prior requirement for a 5 year PIV Card Renewal (FIPS 201-1 Section 5.3.2.1). The addition of this new requirement will require expensive changes to many of the EP laboratory test tools as well as expensive retesting of currently approved vendor FIPS-201-related products. We recommend a restatement of this requirement to allow existing durability testing procedures to remain in place.	Change to: "The credentials and information contained on the PIV Card shall be valid for no more than six years."	Declined. The current durability testing citing ISO/IEC 10373 Parts 1, 3, and 6 is not specific to a 5 year lifetime. The six year timeline has been requested by agencies to synchronize with certificate expiration.
ES-4	Electrosoft Services Inc.	Sarbari Gupta	E	10	548	2.5.2	"Revocation of the Digital Signature Key certificate is only optional if the PIV Card has been collected and zeroized or destroyed. Similarly, the Key Management Key certificate should also be revoked if there is risk that the private key was compromised." The wording is awkward. The critical requirement here is revocation of any certificate that may be compromised.	"The Digital Signature Key certificate shall be revoked, unless the PIV Card has been collected and zeroized or destroyed in which case such revocation shall be optional. In addition, each certificate corresponding to any other on-card private key shall be revoked if there is a risk that the on-card private key is compromised."	Resolved by DOT-15.
ES-5	Electrosoft Services Inc.	Sarbari Gupta	T	11	589	2.5.4	"Communication between the PV Card issuer and the PIV Card shall occur only over mutually authenticated secure sessions between tested and validated cryptographic modules (one being the PIV Card)." This statement makes the status quo a requirement; but how will this requirement be enforced? This type of function has so far been out of scope of SP 800-73-3. It is in scope of FIPS 140-2, but there is typically no method to enforce the presence of a feature like this. This comment also applies to the bullet at line 592.	Keep this statement in FIPS 201-2, but add an Appendix to FIPS 201-2 identifying required PIV Card features or Security Policy content. The Appendix should be in the form of a Security Policy "profile", similar to a Common Criteria Protection Profile for expected features (like this) and dependent algorithms (like SP 800-56A ECC CDH Section 5.7.1.2 if 9D is supported).	Declined to add a profile. Note: Post issuance updates have been requested by agencies. However, since FIPS 201 does not standardize the card management, implementation details of mutually authenticated secure sessions are out of scope.
ES-6	Electrosoft Services Inc.	Sarbari Gupta	T	12	603	2.5.5	See comment re Section 6.2.5. The statement in this section should apply to either PIN or any retry counter for a biometric used as a PIN alternative.	Add a sentence following the first sentence in this section, near the end of line 606: "Similarly, the need to reset authentication data retry counters also applies to any biometric authentication mechanism used as a PIN alternative." Modify the next sentence to read: "PIN **or biometric authentication data retry count** resets may be performed by the card issuer."	Declined -- The second paragraph in Section 2.5.5 (now Section 2.9.4) addresses the requirement for resetting biometric data. These requirements are different from PIN reset and should not be combined.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ES-7	Electrosoft Services Inc.	Sarbari Gupta	E	12	619	2.5.5	"... requiring the termination of PIV Cards that have been locked." In this context, does "locked" mean PUK retries are exhausted? Suggest clarification of this point.	"... requiring the termination of PIV Cards blocked by exhausted PUK retry count." Alternatively, define a term for this in the Glossary; "lock" seems overloaded with several possible meanings including: the low level card transport lock; VERIFY not yet performed; blocked on PIN retry count = 0; blocked on PUK retry count = 0.	Resolved by removing use of word 'locked'.
ES-8	Electrosoft Services Inc.	Sarbari Gupta	T	21	882	4.1.3	"... temperature and humidity-induced dye migration, ..." This section of FIPS 201-2 lumps together issues of card durability ("temperature") with the effects on printing on the card (humidity-induced dye migration"). This particular item is one example of a test that was sorted into the Card Printer Station (CPS) category. The issue of card body qualification and printer effect qualification should be addressed in this version of FIPS 201-2.	Recommend a small group effort to restate this section.	Declined. Printer testing is not covered by this standard.
ES-9	Electrosoft Services Inc.	Sarbari Gupta	T	21	884	4.1.3	"Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water mixture. The reagents called out in Section 5.4.1.1 of [ISO10373] shall be modified to include a two percent soap solution." This statement is obscure and long been the source of confusion, and should be reworded. The hand cleaning requirement and separate statement about exposure to soapy water are essentially redundant.	"Card durability testing shall include contaminant exposure in accordance with [ISO10373] Section 5.4.1.1. In addition to these contaminants, cards shall not malfunction or delaminate after hand cleaning with a two percent soap plus water mixture."	Resolved by removing "The reagents called out in Section 5.4.1.1 of [ISO10373] shall be modified to include a two percent soap solution."
ES-10	Electrosoft Services Inc.	Sarbari Gupta	T	21	915	4.1.3	"The PIV Card may be subjected to additional testing." This sentence is too subjective for the purposes of the GSA FIPS 201 EP, Recommend removing it, or alternately, making it clear that this is out of scope for FIPS 201 EP compliance testing.	Delete this line or restate it as "Departments and Agencies may subject the PIV Card to additional testing beyond that required by this Standard as required to meet their specific use needs."	Out of scope. The need for additional testing may be determined by GSA or individual departments and agencies. There is no reason to call out specific entities in FIPS 201.
ES-11	Electrosoft Services Inc.	Sarbari Gupta	T	37	1141	4.1.6.1	"One or two iris images" is listed as optional, but in several places in FIPS 201-2 and SP 800-76-2, iris image is listed as a mandatory feature to be supported if fingerprint cannot be used. See also line 1132 that lists two iris images. The iris container must be mandatory to support iris as a mandatory backup to fingerprint.	Change to: "One or two iris images that are in addition to the two mandatory biometric fingerprints (i.e., the combination of fingerprints plus iris image(s) is acceptable as an option)"	Declined. Since release of the FIPS 201-2 draft, the decision is that iris is now optional, so this change is not necessary.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ES-12	Electrosoft Services Inc.	Sarbari Gupta	T	37	1142	4.1.6.1	"On-card biometric comparison data" It is not clear in FIPS 201 that there are two different containers for fingerprints; one for on-card, one for off-card. SP 800-76-2 refers to some template differences; and as a container, GET DATA access requires PIN verify while on-card biometric comparison does not.	Change to: "On-card biometric comparison data; note that this data is separate from the other mandatory and optional biometric data elements elsewhere listed"	Resolved by adding a footnote to Section 4.2.3.1: "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]." Also SP 800-76-2 will itself introduce and clarify this topic (why and how the binary representations of the two minutia representations are different). INCITS 378:2004 define the off-card templates and INCITS 19794-2:2011 defines the on-card templates. Semantically the minutiae are very similar; syntactically they are quite different. Both are widely used and implemented commercially.
ES-13	Electrosoft Services Inc.	Sarbari Gupta	T	37	1150	4.1.6.1	"The PIN falls into the first category, the card management key into the second category, and the CHUID, biometric credential, symmetric keys, and asymmetric keys into the third." See comment on 6.2.5. With introduction of on-card biometric comparison, if it is a PIN substitute, biometric is also in the first category.	"The PIN **and on-card biometric comparison data fall** into the first category, the card management key into the second category, and the CHUID, biometric credential, symmetric keys, and asymmetric keys into the third."	Resolved by disposition of IGL-16.
ES-14	Electrosoft Services Inc.	Sarbari Gupta	T	39	1231	4.3	"… keys used to establish a secure messaging …" FIPS 201-2 makes only broad reference to secure messaging, for example use of secure messaging in relation to transfer of on-card comparison biometric data (suggested by SP 800-76-2) and PIN (suggested by line 1500 but not clear if this means physically secure, logically secure, or some combination). This topic merits inclusion of a separate section or paragraph in FIPS 201-2 with a more detailed discussion of secure messaging. For most practical purposes, all cards support secure messaging mechanisms. Identification of the different use cases where secure messaging must or should be employed would be useful.	Add a paragraph (or new section 4.3.1) addressing when secure messaging must be used and where it is recommended that is should be used.	Accept in principle.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ES-15	Electrosoft Services Inc.	Sarbari Gupta	T	40	1236	4.3	"Where digital signature keys are supported, the PIV Card is not required to implement a secure hash algorithm. Message hashing may be performed off card." Per SP 800-73-3, hashing is be performed off card; there is no testing for on-card hashing performance (i.e., cards tested by NPIVP). However, it would be useful to add support for on-card hashing, perhaps in the form of an additional tag. Currently, off-card hashing means the digital signature operation does not support the non-repudiation property. Until PIV, an operation without integral hash was considered by CMVP not to be a true digital signature. Cards have memory limitations, but for some purposes - like signing records by agents - non-repudiation is a useful feature.	Change to: "When applying the digital signature key for signing, the secure message hash function may be performed off card." Add a tag for on-card hash in SP 800-73 and explain in this section 4.3 accordingly.	Declined. As long as off-card hashing is possible, a relying party would not be able to distinguish between a digital signature created using on-card hashing from a digital signature created using off-card hashing.
ES-16	Electrosoft Services Inc.	Sarbari Gupta	T	41	1302	4.3	"Private key operations may not be performed without explicit user action." This is the one place where the PIN ALWAYS is required; it seems much more important to be clear about the meaning of explicit user action here than to state in the PAK and KMK usage explanations what is not required.	"Private key operations shall not be performed without explicit user action - the PIN shall be verified immediately preceding any use of this key."	Resolved by adding reference to NIST IR regarding PIN Caching.
ES-17	Electrosoft Services Inc.	Sarbari Gupta	T	42	1330	4.4	The paragraph starting at line 1330 gives further indication of separate containers for on-card and off-card biometric (see comments for section 4.1.6.1). There are indicators of differences in SP 800-76-2, but it is not clear how this data uses a different on-card template or the same as used for other biometric data.	Please clarify how on-card and off-card biometric data differ. Specifically note any differences in container access control, and where there are differences, if any, in the container for the on-card biometric comparison data.	The restructuring accepted for AMAG-6 means that this clarification is not needed here. It will be clarified in the renumbered section 4 with the text given in ES-12.
ES-18	Electrosoft Services Inc.	Sarbari Gupta	T	43	1351	4.4.1	Use of "TBD" to identify an external specification is not normative and does not support planning. A specific reference is preferable or alternately, language that explicitly indicates that the 'manner and representation' are not required until identification and publication of the external reference.	Consider wording similar to: "A card issuer shall be able to import and export a chain-of-trust in the manner and representation described in TBD once TBD final release occurs.	Resolved by disposition of DoD-53.
ES-19	Electrosoft Services Inc.	Sarbari Gupta	T	47	1500	4.5.4	"If the PIN input device is not integrated with the reader, the PIN shall be transmitted securely and directly to the PIV Card for card activation." This appears to be an option for secure messaging use when PINs are transmitted. This should be further clarified in section 4.3 per comments regarding secure messaging.	Please expand section 4.3 to include a paragraph on secure messaging to include specific use cases for mandatory and recommended secure messaging use.	Declined -- Lines 1499-1501 are unchanged since the original FISP 201 and are not intended to require seccure messaging nor secure session.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ES-20	Electrosoft Services Inc.	Sarbari Gupta	T	51	1621	6.1.1	Relationship to OMB's E-Authentication Guidance The draft SP 800-63 supports OMB M-04-04. Recommend that this section reference SP 800-63 for detailed e-authentication specifications. FIPS 201-2 Appendix E, line 2003 indicates this, but this section 6.1.1 should as well.	Identify relationship to SP 800-63 in this section.	Declined. This reference is redundant since FIPS 201 authentication mechanisms follow SP 800-63 general guidelines.
ES-21	Electrosoft Services Inc.	Sarbari Gupta	T	56	1760	6.2.4.1	"The cardholder is prompted to submit a PIN." If the on-card biometric is indeed a valid PIN alternative, it should be listed here as an alternative for authentication	Include optional use of on-card biometric authentication after this line and after line 1761 (for example, 2a or 2b plus 3a or 3b steps instead of steps 2 and 3)	Resolved by the following changes: - Combine steps 2 and 3. - Add a sentence – If implemented, other card activation mechanisms, as specified in [SP 800-73], may be used to activate the card. - Change the characteristics to - Strong resistance to use of unaltered card by non-owner since card activation is required.
ES-22	Electrosoft Services Inc.	Sarbari Gupta	T	57	1795	6.2.5	"A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC) authentication and the card with an indication of the success of the on-card biometric comparison. The response includes information that allows the reader to authenticate the card. The cardholder PIN is not required for this operation." These sentences do not seem clear that on-card biometric comparison is an alternative to PIN regarding card state. However, SP 800-76-2 is clear, stating on line 325: "Indeed, FIPS 201-2 extends on-card comparison as an alternative to PIN entry in altering the state of the PIV card." This is an important point to be clear on to ensure the GSA FIPS 201 EP has appropriate requirements traceability.	"A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC) authentication and to provide the card with an indication of the success of the on-card biometric comparison. **Successful on-card comparison is an alternative to PIN entry in altering the state of the PIV card.** The response shall include information that allows the reader to authenticate the card; the cardholder PIN is not required for card authentication."	Declined. While card activation may be a side effect of OCC authentication mechanism, this section is specifying an authentication mechanism rather than card activation. See Section 4.1.7.1 (now Section 4.3.1) for alternate ways of activating the card.
ES-23	Electrosoft Services Inc.	Sarbari Gupta	T	57	1792	6.2.5	This section refers to fingerprint biometric but it should also apply to the iris biometric.	Include iris biometric discussion in this section	Resolved by changing 'fingerprint template' with 'on-card biometric comparison data'. However, note that SP 800-76 currently only specifies use of fingerprints for OCC.
ES-24	Electrosoft Services Inc.	Sarbari Gupta	G	?	?	?	Perimeter control devices are in existence - e.g. handhelds. They are not defined as a GSA category because they are not mentioned in FIPS 201-2 documentation.	Add a section defining perimeter control devices and mobile devices that may be used for both physical access control scenarios and logical access control (mobile access to networks).	Declined. FIPS 201-2 specifies a set of authentication mechanisms in Section 6 that may be used for physical and/or logical access, but does not mention nor restrict the types of devices that might implement those authentication mechanisms.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ES-25	Electrosoft Services Inc.	Sarbari Gupta	T	61	1914	A.4	Current wording clarifies the more blanket statement made in FIPS 201-1, but does not address other types of devices that perform crypto. These devices should also have a FIPS 140-2 cert per FISMA (level to be defined).	Convene a small group to address this section. What Level(s) makes sense for each category? By default, GSA Approval Procedures call for Level 1 - this may make sense in some cases. This is an issue worthy of more examination.	Out of scope. The choice of an appropriate minimum Security Level for FIPS 140 validation for cryptographic modules that are not covered by Appendix A.4 is out of scope of FIPS 201-2.
ES-26	Electrosoft Services Inc.	Sarbari Gupta	E	75	2328	F	SP 800-73-3 is cited, but it is not in line with this draft standard. This also pertains to the issue of immediate enforcement of this standard on adoption (see comments for line 169).	See comment for line 169 and include a foot note about SP 800-73-4 and SP 800-85A-3 development, and the short term solution of some card commands in SP 800-76-2 for that line.	Declined. Our intention is to modify all Special Publications related to PIV to account for changes made in FIPS 201-2 in the future and we cannot mention a specific version of an SP, as it might change within the next 5 years.
ES-27	Electrosoft Services Inc.	Sarbari Gupta	E	75	2330	F	SP 800-76-2 is in currently draft, and should be in force when FIPS 201-2 is in force.	Cite SP 800-76-2.	Declined. References will be updated if SP 800-76-2 is completed during the FIPS revision process.
ES-28	Electrosoft Services Inc.	Sarbari Gupta	E	8	476	2.4	"Agencies may reuse them or discard …" Is this policy consistent with page 9 Section 2.5.1 line 519 statement "The original PIV Card must be collected and destroyed"?	"Agencies may reuse or destroy …"	Resolved by Cert-18.
ES-29	Electrosoft Services Inc.	Sarbari Gupta	T	40	1256	4.3	"The key management key is an asymmetric private key supporting key establishment and transport, and it is optional. This can also be used as an encryption key." The key management key is an optional asymmetric private key supporting key decryption (when used with RSA) and shared secret generation (when used with an ECC key to implement the ECC CDH primitive). The key management key is not used to establish keys on the PIV Card.	Please clarify.	Resolved by deleting "This can also be used as an encryption key." Note that the key management key is not used to establish keys on the PIV Card.
ES-30	Electrosoft Services Inc.	Sarbari Gupta	T	11	579	2.5.3	"Only the keys and certificates shall be updated." Shouldn't old certificates be revoked if the corresponding private key is compromised?	"Only the keys and certificates shall be updated, and the certificates corresponding to all compromised keys shall be revoked."	Resolved by adding the following sentence: "If the PIV Authentication key, asymmetric Card Authentication key, the digital signature key, or the key management key, was compromised, the corresponding certificate shall be revoked."
ES-31	Electrosoft Services Inc.	Sarbari Gupta	E	38	1185	4.2	"… (since the digital signature provides entropy equivalent to a password)." Please provide a reference for the source of this statement.	Add a footnote with a reference.	Resolved by Cert-73.
FAA-1	Federal Aviation Administration (AIN-600)	Will Morrison	S	all		Various	Refer to the PIV token as a "PIV Credential"	The terms PIV credential and PIV card are used interchangeably. "Credential" is more appropriate and should be the moniker for the token.	Resolved by WM-1.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FAA-2	Federal Aviation Administration (AIN-600)	Will Morrison	S	5		2.1	Bullet (+) number 2 - Change Verbiage to Read: "A credential is issued only after a National Agency Check with Written Inquiries (NACI) or equivalent (as defined by the Office of Personnel Management (OPM)) is initiated, and the favorable completion of an FBI National Criminal History Check (NCHC)."	Clarification. Better defines what is an equivalent to an NACI, and that a FAVORABLE NCHC check must be completed.	Declined. Current language is consistent with the Springer Memorandum and M-05-24. See OPM-2 for clarification on 'or equivalent"
FAA-3	Federal Aviation Administration (AIN-600)	Will Morrison	S	5		2.1	Bullet (+) number 3 - Change Verbiage to Read: "An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State government photo identification issued to the individual applying for the PIV credential."	Omission of the term "valid" infers that invalid identification documents may be presented. Further, FIPS-201-2 should address the statutory requirements for acceptance of identification that complies with the REAL ID Act of 2005.	Decline to add 'valid' to the sentence since the requirement is specified in 2nd draft of FIPS 201, Section 2.7. Declined to address REAL ID Act of 2005 since FIPS 201 derives source document requirements from Form I-9, which is used by Federal government agencies and departments.
FAA-4	Federal Aviation Administration (AIN-600)	Will Morrison	S	5		2.1	Bullet (+) number 9 - Change Verbiage to Read: "An official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential."	Clarity: Any official, corrupt or not, should not be able to issued or authorize the issuance of a credential to any one with false (or "incorrect") identification or to those not entitled.	Resolved by WM-3.
FAA-5	Federal Aviation Administration (AIN-600)	Will Morrison	S	6		2.2	Include the Springer Memorandum as an appendix to FIPS-201-2.	If FIPS-201-2 is to be the authoritative guidance for PIV cred issuance, it should include such documentation that provides amplifying guidance to PIV cred issuance processes/guidance. Similarly, OMB memoranda that addresses PIV cred issuance (e.g., M-05-24; M-11-11, et alia) should also be included in an appendix with FIPS-201-2	The Springer Memorandum will likely be superseded by OPM's future tiered investigative standard. Memoranda could be amended. Therefore, including these memoranda is not advisable.
FAA-6	Federal Aviation Administration (AIN-600)	Will Morrison	E	All		Various	The terms PIV credential and PIV card are used interchangeably. "Credential" is more appropriate and should be the moniker for the token.	Refer to the PIV token as a "PIV Credential"	Resolved by WM-1.
FAA-7	Federal Aviation Administration (AIN-600)	Myles Roberts	G	All		Various	Use the term "Standard" consistently with the same term in HSPD-12, the document that grants your authority.	Capitalize "Standard" (as does HSPD-12) throughout FIPS 201-2 because it is a defined term.	Accept.
FAA-8	Federal Aviation Administration (AIN-600)	Myles Roberts	G	All		Various	The term "Standard" as used consistently throughout FIPS 201-2 is inconsistent with its definition in the Glossary.	Change the definition of "Standard" in the Glossary to the way that FIPS 201-2 uses it, as the defined set of specific guidelines for PIV Cards, and authentication and authorization processes related to them; or, as the Abstract's first clause defines it, "the architecture and technical requirements for a common identification standard for Federal employees and contractors."	Resolved by deleting definition of "Standard" from the Glossary.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FAA-9	Federal Aviation Administration (AIN-600)	Myles Roberts	G	ii	1		NIST should get contributions from the Interagency Security Committee (ISC). EO 12977 created the ISC to address continuing government-wide security for federal facilities. enhance the quality and effectiveness of physical security in, and the protection of buildings and civilian federal facilities in the United States. The ISC standards apply to all civilian federal facilities in the United States.	Contact ISC@dhs.gov and work with them on consistent recommendations for Physical Access Control Systems such as in section 6 (and section 3.1.3). See http://www.dhs.gov/files/committees/gc_1194977813020.shtm	Noted. Please consider that Section 6 of FIPS 201-2 specifies a set of authentication mechanisms, not recommendations for Physical Access Control Systems.
FAA-10	Federal Aviation Administration (AIN-600)	Myles Roberts	E	iii	16	Abst	If you list many SP 800 series, list all applicable SP 800s and expressly state that NIST may add more in the future. If you omit any relevant to PIV, expressly state the rationale for listing some and omitting others. Explain how agencies know whether an SP 800 series is included in the "Standard" or not. Expressly state that the Standard includse all SP 800 series--or at least those relevant to PIV.	Exressly define the Standard as including not only FIPS 201 but also applicable guidelines in the SP 800 series. For example, add "The requirements for physical access control systems are specified in Special Publication 800-116…"	Resolved by adding SP800-96, SP 800-156, and SP 800-157. Also, add these in Appendix D.
FAA-11	Federal Aviation Administration (AIN-600)	Myles Roberts	E	iv	21		HSPD-12 is the authoriative document. FIPS 201-2 should use consistent references to corresponding language in it.	Change the plus marks (+) for each bullet point to correspond with the authoriative document: HSPD-12 that uses (a) through (d) in its ¶3.	Accept.
FAA-12	Federal Aviation Administration (AIN-600)	Myles Roberts	E	iv	27		This modifying phrase was only relevant during the grace period in 2004 and 2005. The grace period has long expired. Also, use active voice and quotes to maintain HSPD-12 as direct source of authority.	Delete "As promptly as possible, but in no case later than eight months after the date of promulgation," Instead, Begin sentence with "HSPD-12 requires executive departments and agencies to…" Use quotes to show you arr directly quoting from HSPD-12 ¶4.	Resolved by GSA-1.
FAA-13	Federal Aviation Administration (AIN-600)	Myles Roberts	E	iv			As this FIPS 201-2 is an update, at the end of "3.Explanation," or in a footnote, cite the section of HSPD-12 that provides for updates.	Add quote from HSPD-12 ¶2, "The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies."	Declined. The Qualifications section (Section 11 of the Announcement) addresses this.
FAA-14	Federal Aviation Administration (AIN-600)	Myles Roberts	E	v		8	Clarify that NIST is not revoking the option of an Agency to self-accredit itself as an Issuer; and that existing self-accredited issuers under SP 800-79-1 remain valid.		Noted. As per OMB, the agency can continue to self-accredit according to SP 800-79. In future, 3rd party accreditation review may be required by OMB.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FAA-15	Federal Aviation Administration (AIN-600)	Myles Roberts	E	vi		9		Reiterate or cite an internal section to remind the reader the effective date for WHAT. In order words, if pp9 re Effective Date says departments and agencies must comply with the Standard, point them to the Standard.	Declined. "This Standard" refers to FIPS 201-2.
FAA-16	Federal Aviation Administration (AIN-600)	Will Morrison	T	5	360	2.1	Clarification. Better defines what is an equivalent to an NACI, and that a FAVORABLE NCHC check must be completed.	Bullet (+) number 2 - Change Verbiage to Read: "A credential is issued only after a National Agency Check with Written Inquiries (NACI) or equivalent (as defined by the Office of Personnel Management (OPM)) is initiated, and the favorable completion of an FBI National Criminal History Check (NCHC)."	Current language is consistent with the Springer Memorandum and M-05-24. See OPM-2 for clarification on 'or equivalent"
FAA-17	Federal Aviation Administration (AIN-600)	Will Morrison	T	5	362	2.1	Omission of the term "valid" infers that invalid identification documents may be presented. Further, FIPS-201-2 should address the statutory requirements for acceptance of identification that complies with the REAL ID Act of 2005.	Bullet (+) number 3 - Change Verbiage to Read: "An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State government photo identification issued to the individual applying for the PIV credential."	Resolved by FAA-3.
FAA-18	Federal Aviation Administration (AIN-600)	Will Morrison	T	5	372	2.1	Clarity: Any official, corrupt or not, should not be able to issued or authorize the issuance of a credential to any one with false (or "incorrect") identification or to those not entitled.	Bullet (+) number 9 - Change Verbiage to Read: "An official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential."	Resolved by WM-3.
FAA-19	Federal Aviation Administration (AIN-600)	Will Morrison	T	6	380	2.2	If FIPS-201-2 is to be the authoritative guidance for PIV cred issuance, it should include such documentation that provides amplifying guidance to PIV cred issuance processes/guidance. Similarly, OMB memoranda that addresses PIV cred issuance (e.g., M-05-24; M-11-11, et alia) should also be included in an appendix with FIPS-201-2	Include the Springer Memorandum as an appendix to FIPS-201-2.	The Springer Memorandum will likely be superseded by OPM's future tiered investigative standard. Memoranda could be amended. Therefore, including these memoranda is not advisable.
FAA-20	Federal Aviation Administration (AIN-600)	Myles Roberts	T		877-892	4.1.3	PIV must be more durable to withstand multiple insertions and withdrawals daily into LACS and PACS. Real-world experience suggests an average life of 18 months rather than 60 months.		Noted. The six year timeline has been requested by agencies to synchronize with certificate expiration. See DOT-12 and ES-3.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FAA-21	Federal Aviation Administration (AIN-600)	Myles Roberts	T		1339 - 1415	4.4.1	If NIST states its assumption, their requirement to store fingerprints might make more (or less) sense. I offer no comment on whether it's justified. Q: Is (a) or (b) the greater risk (liklihood x damage)? (a) Social Engineering: an attacker stealing someone else's identity during subsequent Enrollment or Issuance by a facility's security assistant (e.g., secretary, receptionist); or (b) Hacking: an attacker copying, altering or deleting the fingerprints in a FIPS 140-2 database (maintained by the best contractors lowest bids can buy)?	At the very least, NIST should explicitly state its underlying assumption that justifies storing fingerprints. The assumption seems to be that reducing risk of identity theft via social engineering is worth increasing risk of storing fingerprints in a database off the card.	Declined. Chain-of-trust provides cost savings to agencies by reusing previous enrollment record, and all of the data stored in agency systems is subject to FISMA.
FAA-22	Federal Aviation Administration (AIN-600)	Will Morrison	T		1339 - 1415	4.4.1	Do not allow the storage of fingerprint minutia within the IdMS or any other DB for any period longer than to encode the data on the card.	Loss risk of privacy data is too great to store the FP minutia on the card. The ability to reconstruct a fingerprint from minutia has been published in the wild. A cracker could easily access an IdMS DB holding FP minutia and reconstruct the FP. The convenience provided does not outweigh the risks of compromise.	Declined. All data is subject to appropriate controls through FISMA. Add reference to FISMA in appendix.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FE-1	federal employee	Jeni Cook	G	p. 8. Add section for "Professional Name" after Pseudonyms"		2.4	I affirm that there is a critical need for Homeland Security to protect the safety of the American people and the security of the federal government's resources. I believe this can and should be accomplished without impinging on the private lives of federal employees. The Problem: There are many women (and possibly some men) who use a "professional name" as well as a "family name." There are a variety of reasons for this: some professional in nature, some related to safety and security issues, some are more personal or individualized reasons. (Were it not for the fact that I believe you want brevity, I would give examples of all three. Please contact me by phone if hearing examples might influence the determination of this matter.) Some federal employees have used both names (one at work, the other in non-government, private life) for years without problem or incident. (In my case, I have done so for 30 years.) The professional name is similar to a "stage name" or a "pen name." The problem now arises (in the PIV identity proofing and registration requirements) that the two forms of identification acceptable as primary identification (driver's license and passport) are both in the form of the private, family name. A birth certificate is available in the professional name. The social security identification is available in the professional name, but since neither driving nor international travel is associated with the professional career, both the driver's license and passport have been obtained in the family name. Of course, I cannot speak for all employees who use a professional name. However, most of us are not hiding anything. I will use my name as an example. Professionally, I have been known in the Department of Veterans Affairs (for 28 years) and prior to that in the Bureau of Prisons (2 years) as Chaplain Jeni Cook. In my private life, I go by Jeni Cook Furr. Recently, when my multiple background investigations were discovered to be missing in the new electronic OPF, I was happy to give both names for the NACI re-investigation. Both names were again cleared on April 11, 2011. For 30 years I have submitted W-2 forms to the IRS that show the employee name to be Jeni Cook. However, every year, I file my taxes jointly with my husband, and I sign my name on the return form as Jeni Cook Furr. Both names belong to me, and I am one and the same person. My local PIV card issuer said he was unable to proceed in producing my PIV card because my primary identification (driver's license) added the name "Furr" to my employee name, Jeni Cook. I was told I would be required to change my employee name in Human Resources, or the name on my driver's license and/or passport to make them an exact match. Neither option is a good one. Why?	The draft of FIPS 201-2 already comes very close to resolving this problem in 2.4.1, Pseudonyms. The difference between the professional name and the pseudonym is that the employee using a professional name usually is quite willing to provide the private name. In fact, the *need* of this employee is for the government to do the name-matching and recognize that he/she is one and the same person. This matching can be easily accomplished through a variety of means: Matching W-2 forms with tax return documents and signature (usually filing jointly) - Same Social Security number -Facial recognition between PIV and driver's license pictures -Same finger prints -Same iris image -Same hand writing in signatures (In my case, one signature is contained in the other.) - In some cases, matching marriage license to birth certificate. It should be required that the employee provide both names for the NACI and that both names be cleared by the investigation. I am sure that there is already a way to identify the difference between two employees who have a common name (e.g., Mary Lou Jones). There must also be a way to identify the fact that two names refer to the same person. If there is concern that the employee's private name could be fraudulently used through stolen identity, a block could be placed on both names being issued a PIV card *at the same time*. However, it would be critical to ensure that any such block ***not*** trigger placement of either name on a government watch list!	As per OMB policy guidance, a legal name as found in the source documents shall be used.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FE-1 (cont'd.)	federal employee	Jeni Cook	G	p. 8. Add section for "Professional Name" after Pseudonyms"		2.4	1) Many employees request that their name be changed. This is clearly not the same situation. I do not want my employee name changed. After 30 years, that would be a significant waste of government resources (one of the goals of the new PIV card is to increase government efficiency) and cause unnecessary confusion. It would require changing my name on retirement accounts, TSP accounts, the PAID system, My Pay account, health and dental insurance accounts, FSAFEDS account, employee education accounts, government travel accounts and employee travel card, Federal Credit Union Account, USA Staffing account, eOPF, VISTA account, My HealtheVet , just to name those that come to mind first. How much might all of this actually cost the government? Additionally, such a forced employee-name-change would require a change in my government email account. Since I work in a national office and with professionals across the country, it would require more time wasted in explaining who I am, and why I now have a different email account. (No, I didn't request it. No, I'm not recently married, etc.) My professional name is my expression of who I am on the job. It is also how those with whom I associate professionally identify me. The HSPD-12 "Rolling Out" instructions say that steps must be taken to make sure the application process is not disruptive for employees. A forced professional name change would be excessively disruptive for the employee and the day-to-day operations of a national program in the federal government. 2) On the other hand, if I am forced to change the name I use in my family and private life, there will be a personal expense incurred for these changes, and I may also be required to change my name on other personal investments, personal credit cards and personal checking and savings accounts, etc. Being forced to change my private, family name will create the same kind of havoc and confusion in my private life, as changing my professional name would cause in my work life. HSPD-12 says that the "directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans." Furthermore, one of the stated priorities of the FIPS 201 policy is to protect personal privacy of employees. Requiring an employee to change his/her identity used in private life certainly seems to violate that stated value. I have no plans to pursue this type of violation through other channels, but it would be wise to consider this implication proactively. It is likely that some employees will pursue it since the current policy will also have a disproportionate impact upon women.		

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
FSATO-1	Federal Student Aid Technology Office	Marcus Williams	T	20	851	4.1.2		Section 4.1.2 of fips201-1 should include ink resistant polymer coatings	Declined. The list provided are examples and agencies are not precluded to use other security features.
GSA-1	GSA MSO	Bill Windsor	G	iv	118	3	Requires implementation no later than eight months after date of promulgation - later section indicates that OMB will provide guidance on implementation requirements	Determine which is the requirement	Resolved by replacing "As promptly as possible, but in no case later than eight months after the date of promulgation, executive departments and agencies are required to implement the standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities and logical access to controlled information systems." with "Executive departments and agencies are required to implement the Standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities and logical access to controlled information systems."
GSA-2	GSA MSO	Bill Windsor	G	3	Multiple	1.4	If a normative section references an information section - does that make the informative section now "normative" - and vice versa, for example - [see section 2.3, 2nd bullet, section 2.5.6 last sentence] [see section 3.1 and 3.1.3 references to section 6]	Need clarification of the requirements	Declined. Sections that are marked as informative are informative. An informative reference in a normative section does not make the referenced section normative. Similarly, an informative reference in an informative section to normative text does not change the normative text from being normative to being informative.
GSA-3	GSA MSO	Bill Windsor	G	Multiple	Multiple	Multiple	Reference is made to several PKI certificate requirements - which are defined and proscribed by the Federal PKI Policty Authority (FPKIA). Requirements and guidelines from the FPKIA change frequently in response to the changing PKI technologies and implementations by Federal agencies.	NIST should reference the applicable FPKIA policy documents or define NIST PKI guidelines document (800 series).	Declined to define a PKI guideline document (800-series). FIPS 201-2 is already referencing the applicable FPKIPA requirements.
GSA-4	GSA MSO	Bill Windsor	G	Multiple	Multiple	Multiple	PKI-Auth is used in some cases and PIV authentication is used in others. Differences in meanings and useage are not clearly understood.	Be consistent in reference ot the PIV authentication PKI certificates.	Noted. PKI-AUTH is an authentication mechanism that makes use of the PIV Authentication certificate and the PIV Authentication key.
GSA-5	GSA MSO	Bill Windsor	T	7	381	2.3	Identity documents approved for acceptance have a tendency to change	Suggest referencing another document or creating a guidelines document that supports change.	Resolved by Cert-10.
GSA-6	GSA MSO	Bill Windsor	T	7	441	2.3	A new chain-of-trust record shall be created in accordance with Section 4.4.1 for the applicant. References Section 4.4.1 [Lines 1340-1342] - The chain-of-trust is a sequence of related enrollment data records, and shall be created and maintained through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records.	A new chain-of-trust record shall be created for the acquisition and maintenance of enrollment data for each applicant is created.	Resolved by AMAG-6.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
GSA-7	GSA MSO	Bill Windsor	T	8	478	2.4.1	Pseudonyms - this may impact USAccess processing related to 1:N duplication checks, if an individual has more than identity in the system May impact agency systems if inter-agency exchange of data occurs.	Employing agencies must to be aware that employees being authorized to be issued a new PIV card using a pseudonym may need to have any other records within the same or associated PIV identity managements removed or otherwise protected from being divulged to unauthorized individuals because of a 1:N fingperprint duplication check that might occur.	Out-of-Scope. These types of implementation details should be communicated by the issuers to their customers.
GSA-8	GSA MSO	Bill Windsor	T	9	491	2.4.2	Grace period - Doesn't seem consistent with intent - issue a new PIV card with initial PIV issuance requirements? Are affiliation changes a part of this? Is the intent that this is NOT a re-issuance?	Need clarification whether the intent was issuance or re-issuance for this use case.	Resolved by Cert-20.
GSA-9	GSA MSO	Bill Windsor	T		515	2.5.1	Could a trusted agent update the chain-of-trust and then renewal proceed without requirement for re-enrollment and new card?	Need clarification	Resolved by DOT-18.
GSA-10	GSA MSO	Bill Windsor	T	9	517	2.5.1	Allowance for renewal starting 12 weeks rior to expiration of a valid PIV card - is this enough time for large IDMS systems, such as USAccess.	Could the allowance period be longer, such as 6 months?	Resolved by DHS-4.
GSA-11	GSA MSO	Bill Windsor	T	10	530	2.5.1	Does not specifically state that the key management certificates may be imported to the renewed PIV card, but does not specifically state the the expiration date of the certificate shall not exceed the the expiration date of the card, as it does for the other 3 certificates.	Need to clarify whether the "current," [not key histories/certificates] key management certificate can exceed the life of the card.	Declined. It is possible to have key management key expiration exceed the life of the card; however, management of the certificates will be simpler if they have the same lifetimes.
GSA-12	GSA MSO	Bill Windsor	T	10	547	2.5.2, 2.5.2.1	This section does not address the certificate revocation requirements when a "name change"occurs -	Need to clarify whether this requirement is for just compromise…	Resolved by DOT-15.
GSA-13	GSA MSO	Bill Windsor	T	11	577	2.5.3	Re-key for card or system compromise.	Need clarification if this also includes "routine" re-key for certificate updates as found in section 2.5.4	Resolved by Cert-38.
GSA-14	GSA MSO	Bill Windsor	T	11	584	2.5.4	What is the reason the FASC_N shall not be modified by a post issuance update?	Need clarification.	Declined. The FASC-N is intended to uniquely identify the card, which would not be the case if the value could be changed in a post-issuance update.
GSA-15	GSA MSO	Bill Windsor	T	11	596, footnote 2	2.5.4	There are situations where Internet connectivity may cause a session to timeout and/or stop full activation - that could be a "failure" to complete a post issuance update. These sessions and activities may be re-started in many cases.	Need clarification of whether a re-try for an interrupted update could be done under some circumstances.	Resolved by DoD-27.
GSA-16	GSA MSO	Bill Windsor	T	12	603	2.5.5	"or require the cardholder to provide a primary identity source document (see Section 2.3)." Capture or recording of identity source documentation prior to verification data reset not required.	In the event identity source documentation is provided in lieu of biometric match to chain of trust, that identity source documentation must be recorded (See Section 2.3.)	Declined: A second primary ID source document is required in order to align with ID proofing requirements at issuance. Capture or recording of identity source document is not necessary.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
GSA-17	GSA MSO	Bill Windsor	T	12	616	2.5.5	If a biometric match is performed - then the type of biometric used for the match shall not be the same as the type of biometric data that is being reset.	Need clarification on this. Can a picture on the outside of a card be used to update the picture? Can a fingerprint check against the card or IDMS be used to update fingerprints?	Off-card fingerprint comparison cannot be used when resetting the on-card fingerprint templates. This comment is resolved by replacing the 2nd paragraph of Section 2.5.5 (now Section 2.9.4) with the following: Verification data other than the PIN may also be reset (i.e., re-enrollment) by the card issuer. Before the reset, the issuer shall perform a 1:1 biometric match of the cardholder to reconnect to the chain-of-trust. The type of biometric used for the match shall not be the same as the type of biometric data that is being reset. For example, if fingerprint templates for on-card comparison are being reset, then a 1:1 iris match could be used to re-connect to the chain-of-trust. If no alternative biometric data is available, the cardholder shall provide the PIV Card to be reset and another primary identity source document (as specified in Section 2.7). An attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the PIV Card. New verification reference data shall be enrolled. The PIV Card's activation methods associated with the verification data shall be reset and the new verification data shall be stored on the card. Departments and agencies may adopt more stringent procedures for verification data reset (including disallowing verification data reset); such procedures shall be formally documented by each department and agency.
GSA-18	GSA MSO	Bill Windsor	T	13	638	2.5.6	Agencies are not required to revoke digital signature keys and key management key on card termination.	Need clarification on this - is this related to exporting those keys and certificates based on policy?	Noted. In cases where the card has been collected and destroyed, and there is no potential for misuse of the private key, a decision may be made not to revoke the certificates in order to reduce the size of CRLs. Section 4.9.3 of he "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON] says: "Where subscribers use hardware tokens, revocation is optional if all the following conditions are met: o the revocation request was not for key compromise; o the hardware token does not permit the user to export the signature private key; o the subscriber surrendered the token to the PKI; o the token was zeroized or destroyed promptly upon surrender; o the token has been protected from malicious use between surrender and zeroization or destruction. In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
GSA-19	GSA MSO	Bill Windsor	T	22…	916 and others	4.1.4	Could zone 3F be split to allow an additional line of name data with the ERO being the lower half of the zone?	See Zone 3 PIC attached to these comments.	Declined. Extending Zone 2F would overlap with a number of other zones such as Zones 3F, 6F, and 17F.
GSA-20	GSA MSO	Bill Windsor	T	23	943..	4.1.4.1	What is the requirement for middle initial - is something required (i.e., nmn)?	Need clarification.	Resolved by adding an example in Table 4-1 that shows full name of a person who does not have middle name. Add the following example as the first row in the table: John Doe - DOE, JOHN. Also add characteristics - “simple full name of individual who does not have a middle name.”
GSA-21	GSA MSO	Bill Windsor	T	36, 37, and others	1131, 1141, and others	4.1.6.1 and others	collection of iris images is mentioned as both mandatory and optional.	Need clarification where iris image capture can be optional (i.e., when fingerprints are captured).	The requirement to collect iris if fingerprints were unavailable has been removed per DOJ-10. Since release of the FIPS 201-2 draft, the decision is that iris is now always optional.
GSA-22	GSA MSO	Bill Windsor	T	37..	1158..	4.1.7.1 and others	It would be helpful to have a table similar to the one in Appendix C that clearly defines which data objects and operations are to be available via contact vs. contactless access, as well as with and without cardholder activation.	Need clarification on contact vs contactless access and cardholder activation requirements.	Out of scope. Table 1, Data Model Containers, in SP 800-73 already provides such information. SP 800-73 will be updated to reflect changes in FIPS 201-2.
GSA-23	GSA MSO	Bill Windsor	T	43	1350	4.4.1	Import and export of chain-of-trust requirements not defined.	Need to define those in this document or reference another document.	Resolved by DoD-53.
GSA-24	GSA MSO	Bill Windsor	T	43	footnote 13	4.4.1	If an agency is unable to collect fingerprint or iris, then reissuance would force a new chain-of-trust to be created, implying a new FBI Criminal History Check.	Need clarification whether a new FBI criminal history check is required [terminology of "implying" needs clarification]	Resolved by DoD-54.
GSA-25	GSA MSO	Bill Windsor	T	48	1503	5	PIV Key Management Requirements - there are a lot of technical PKI and key management details in this section that are highly subject to change.	Suggest referencing the Common Policy or creating a NIST guidelines document that supports change.	Declined. This section includes those requirements for which deferral to the Common Policy was deemed inappropriate, and it is not highly subject to change. This information is not appropriate for any current Special Publication, and creation of a new Special Publication that would contain only the information currently in Section 5 would be unwarranted.
GSA-26	GSA MSO	Bill Windsor	T	49	1550	5.4	This specification imposes no requirements on digital signature or key management certificates issued by legacy PKIs	Does this statement apply only toe OIDs used in legacy PKIs or to all PKI certificate requirements?	This statement does not only apply to the OIDs asserted in digital signature and key management certificates issued by legacy PKI, as FIPS 201-2 imposes no requirements on digital signature or key management certificates issued by legacy PKIs.
GSA-27	GSA MSO	Bill Windsor	T	56	1756	6.2.4	The PKI-Auth shall be the alternative authentication mechanism, in cases where neither the fingerprints nor its alternative iris images could be collected for on-card storage	Need clarification where the card authentication asymmetric mechanism could be used.	Resolved by deleting last sentence from Section 6.2.4 (now Section 6.2.3) and changing last two sentences of first paragraph (now a footnote) in Section 6.2.3 (now Section 6.2.1): "As noted in Section 4.2.3.1, neither the fingerprint template nor the iris images are guaranteed to be present on a PIV Card, since it may not be possible to collect fingerprints from some cardholders and iris images collection is optional. When biometric authentication cannot be performed, PKI-AUTH is the recommended alternate authentication mechanism."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
GSA-28	GSA MSO	Bill Windsor	T	64	1276, 1958	D.2	NACI indicator requirements appear to be inconsistent -	Two sections should state same requirement.	As per ICAMSC-111, the NACI indicator will remain a requirement as previously specified in FIPS 201-1. Language in line 1276 and line 1958 will change accordingly.
GSA-29	GSA ICAM Division	Phil Ahn	G	9		2.5.1	The abillity to only renew expiring cards 12 weeks out might not be enough time.	Is there an ability to take it out longer? Maybe 6 months out and let the agencies decide.	Resolved by DHS-4.
GSA-30	GSA ICAM Division	Phil Ahn	G	9		2.5.1	During a card renewal 12 weeks prior to card expiration, can the card and certificates stay active until the new card is activated?	Need the abillity to keep the card and certificates active. This will keep workers using the current cards for physical and logical access until the new cards are available for activation to keep workers operational.	Resolved by DOJ-4. Note that the card and certificates cannot stay active after the card expiration.
GSA-31	GSA ICAM Division	Phil Ahn	G	10		2.5.2	Certain aspects of Card Reissuance described should be an renewal	People should not have to go through the reissuance process if renewal is available. Lost, stolen, and damaged are good examples of a renewal since once the new card is obtained, the employee will have to do a fingerprint validation to activate the card.	Resolved by DOT-15. Reissuance requires revocation procedures while renewal does not. Reissuance is the proper procedure for lost, stolen, or damaged cards.
GSA-32	GSA ICAM Division	Phil Ahn	G	23-24		4.1.4.1	Need more information about when someone does not have a middle name (is it left blank or NMN) and what about where suffixes will be shown.	Need more information	Resolved by adding an example in Table 4-1 that shows full name of a person that does not have middle name. Add the following example as the first row in the table: John Doe - DOE, JOHN. Also add characteristics - “simple full name of individual who does not have a middle name.” Resolved by clarifying that suffix belongs to the secondary identifier as follows: "Names in the Primary Identifier and the first name in the Secondary Identifier shall not be abbreviated. Other names and conventional prefixes and suffixes, which shall be included in the Secondary Identifier, may be abbreviated."
GSA-33	GSA ICAM Division	Phil Ahn	G	36, 37, etc		4.1.6.1, etc.	Iris images were mentioned. What is the point of Iris images…are agencies going to need to be able to validate cards by iris images?	Need more information on what agencies would be responsible for in accepting iris images.	Iris images are now optional. They are well suited to biometric authentication generally and were proposed to handle the unavailable-fingerprint case. Agencies electing to use iris biometrics would have similar responsibilities as they do for fingerprints, or face, today.
IBIA-1	International Biometrics & Identification Association	Walter Hamilton	G			General	The use of the term "On-Card Biometric comparison" or "OCC" is confusing and inconsistent with the term that is most recognizable in the industry - which is “match on card”. Match on card is already referenced in two NIST publications (NISTIR 7477 and NISTIR 7452) and is commonly used by manufacturers as well as in industry and academic publications as a generic term. IBIA believes that it is unnecessary and confusing to introduce terminology that conflicts with accepted norms.		Solved by IBIA-1b below.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IBIA-1b	IBIA	Walter Hamilton	E	2	274	1.3.3	The use of the term "On-Card Biometric comparison" or "OCC" is confusing and inconsistent with the term that is most recognizable in the industry - which is “match on card”. Match on card is already referenced in two NIST publications (NISTIR 7477 and NISTIR 7452) and is commonly used by manufacturers as well as in industry and academic publications as a generic term. It is unnecessary and confusing to promote terminology that conflicts with accepted norms. IBIA does not believe that the specific phrase "match on card" is a vendor trademarked term.	Change "on-Card Biometric comparison" and "OCC" to "match on card" and "MOC". Note, that "match on card" should generally not be capitalized. This change will impact other sections of FIPS 201-2	Declined. Today's biometric standards documents (e.g., ISO/IEC 24787 and ISO/IEC 19795-7) use the term "on-card comparison" replacing the older term "match-on-card".
IBIA-2	IBIA	Walter Hamilton	E	9	484	2.4.1	An open parenthesis is missing in the sentence.	Add an open parenthesis before the word "which."	Resolved by NIST-58.
IBIA-3	IBIA	Walter Hamilton	G	9	514	2.5.1	The minimum accuracy requirements for biometric matching using iris recognition technology will be specified in SP 800-76-2. FIPS 201-2 needs a supporting reference for minimum accuracy for biometric matching using iris recognition technology.	Update FIPS 201-2 to reference SP 800-76-2.	Declined, the main text of FIPS 201-2 refers to [SP 800-76], and this is defined in the references section as meaning SP 800-76-1 or as amended.
IBIA-4	IBIA	Walter Hamilton	G	37	1142	4.1.6.1	The standard should allow PIV issuers to choose an alternative biometric authentication method with the related biometric data stored in the PIV card. This will allow agencies to choose a given biometric method in their own environment without disturbing the global interoperability of the PIV system. Examples could include the use of alternative biometrics like vein pattern recognition or the use of proprietary template extensions to fingerprint and other biometric modalities that will enhance performance.	Suggested text to be added after line 1142 as a new bullet: + Data containers reserved for data objects specific to the PIV card issuer (e.g., for operational biometrics).	Declined. Allowing arbitrary alternative modalities would allow agencies to actively use biometrics instead of those explicitly provided by FIPS 201. The provision in PIV for fingerprint, face, and iris biometrics is intended to realize not just federal interoperability, but also to accrue benefits of standardization, quantitative testing, and marketplace maturity and size. More generally OMB M-11-11 instructs "Agency processes must accept and electronically verify PIV credentials issued by other federal agencies."
IBIA-5	IBIA	Walter Hamilton	T	37	1161	4.1.7.1	This section states that "Other card activation mechanisms, only as specified in [SP 800-73], may be implemented and shall be discoverable."	It is recommended that biometric match on card be included as a user-based cardholder activation mechanism and included in a future version of SP 800-73.	Noted, see disposition of PB-2.
IBIA-6	IBIA	Walter Hamilton	T	39	1232	4	This section refers to "keys used to establish a secure messaging" which can be performed over the contactless interface.	It is recommended that biometric match on card, when implemented over the contactless interface, require secure messaging to protect the privacy of the contactless transmisson of the cardholder's presented template from the reader to the card. It is assumed that such an implementation will be further specified in a future special publication.	See SCA-41.
IBIA-7	IBIA	Walter Hamilton	G	51	1587	6	Use case examples shown in Section 6 are not inclusive of all possible use cases. It would be more appropriate to describe these use cases in a special publication that could be updated more frequently to reflect new use cases.	Move Section 6 content into a special publication that can provide more examples and be more easily updated in the future.	Declined per SCA-53.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IBIA-8	IBIA	Walter Hamilton	E	57	1800	6.2.5	The word "if" is misspelled	Correct spelling	Accept.
IBIA-9	IBIA	Walter Hamilton	E	69	2106	Apdx.E	Neither "match on card" nor "on-card biometric comparison" are included in the glossary.	Add "match on card" to the glossary (see comment 1 above)	Declined, instead add OCC per definition in SCA-98.
ICAMSC-1	ICAMSC	CRFroehlich	T	iii	69	Abstract	Technical interoperability involves more than physical card specifications; it involves the underlying PKI certificates that verify the card, verify the card holder, and may eventually verify the card holder's physical and logical access authorizations. Until that fact is recognized and consistently promulgated -- even in the Abstract -- the PIV Card will never be more than a flash pass outside a parent agency.	Address PKI requirements, policy, and standards in the Abstract.	Declined. The Abstract describes what is specified in FIPS 201 and related Special Publications. PKI requirements, policy, and standards are generally only referenced in these documents.
ICAMSC-2	ICAMSC	CRFroehlich	G	iii	82-83	Abstract	If FIPS 201-2 is going to identify what it is not going to address, it should mention PIV - Interoperable cards as well.	Recommend adding: "This standard also does not specify acceptance policies or requirements for PIV Interoperable or similar identity cards by Federal departments and agencies."	Declined. It is already implicitly stated that PIV-I is out of scope since the Abstract says that "This Standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors." PIV-I does not fit that description.
ICAMSC-3	ICAMSC	CRFroehlich	E	iii	85-87	Abstract	The PIV card is dependent on public key infrastructure for inter-agency interoperability.	Recommend adding: "public key infrastructure" and "PKI."	Accept.
ICAMSC-4	ICAMSC	Steve Howard	T	46	1466-1477	4.5	All reader specifications and requirements should be in [SP800-96].	Replace with: "The minimum requirements for contact and contactless card readers are specified in [SP800-96].	Resolved by Cert-96.
ICAMSC-5	ICAMSC	Steve Howard	T	47	1496-1501	4.5.4	There is real concern around Advanced Persistent Threat that card activation data (both PIN and livescan bio) can easily be compromised.	This section should recommend integrated devices not part of a PC for all card activation. Lines 1499-1501 seem to imply a secure session. Suggest including this in SP800-96	Declined, however, additional text is provided in DoD-55 resolution.
ICAMSC-6	ICAMSC	Steve Howard	T	vi	162		Conformance test only lists SP 800-73	Must also have conformance to 800-78 and 800-76. In particular, testing for 800-78 is specifically the behavior of the card-edge for crypto services, and 800-76 has card-edge bio MOC added.	Resolved by noting that GSA is testing the conformance of PIV Card data objects. Replace "[SP 800-73]" with "[SP 800-73] and [SP 800-78]" Add at or below line 162: "The U.S. General Services Administration (GSA) has set up the FIPS 201 Evaluation Program to evaluate conformance of different families of products that support the PIV processes of this standard - see Appendix A.5."
ICAMSC-7	ICAMSC	Steve Howard	E	vi	164		"…provides an implementation oversight of this standard."	"…provides implementation oversight for this standard."	Accept.
ICAMSC-8	ICAMSC	Steve Howard	E	vi	191		"…technology, the NIST…"	"…technology, NIST…"	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-9	ICAMSC	Jonathan Shu	G	1	230	1.2	Although I agree with the removal of PIV-I and PIV II from the document, and agree that requirements for PIV-Interoperable should be detailed in the FBCA CP, FIPS-201 should include accommodations for agencies who have implemented electronic validation and who can register PIV-Interoperable credentials and link them to successful completion of a NAC-I to allow their affiliates who have PIV-Interoperable credentials to use them instead of having to issue a PIV card.	Recommend add the following text to Section 1.2: Federal agencies who have processes in place to electronically authenticate credentials that have been issued by providers certified by the Federal PKI Policy Authority as compliant with the PIV-Interoperable standard (add footnote to PIV-I for NFI link http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf) may register PIV-I credentials in lieu of PIV credentials provided that access attributes such as successful completion of a NAC-I can be also be electronically validated.	Declined. HSPD-12 specifies "secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)." The use of externally issued PIV-I credential as a replacement for the PIV card, therefore, is not the intent of HSPD-12.
ICAMSC-10	ICAMSC	CPWG	T	1	231-235	1.2	FIPS-201-2 should indicate that PIV-I plus a favorably adjudicated background investigation (minimum NAC-I) is acceptable for contractors in place of a PIV Card	Amend Scope on lines 231-235 to say that "PIV-I plus a favorably adjudicated background investigation (minimum NAC-I) is acceptable for contractors in place of a PIV Card"	Declined. HSPD-12 specifies "... secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)." The use of externally issued PIV-I credential as a replacement for the PIV card, therefore, is not the intent of HSPD-12.
ICAMSC-11	ICAMSC	Steve Howard	T	2	243	1.2	"This standard defines authentication mechanisms offering varying degrees of security." is not clear with regard to both logical and physical access gaining equal weighting in this standard.	Proposed text: "This standard defines authentication mechanisms offering varying degrees of security for both logical and physical access applications."	Accept.
ICAMSC-12	ICAMSC	CRFroehlich	G	2	248-249	1.2	This standard should also exclude the PIV-Interoperable (PIV-I) card.	Recommend adding: "This standard also does not specify acceptance policies or requirements for PIV Interoperable or similar identity cards by Federal departments and agencies."	Declined. It is already implicit from the Scope section that PIV-I is out of scope, as it indicates that the Standard defines the technical requirements for identity credentials issued by Federal departments and agencies to Federal employees and contractors.
ICAMSC-13	ICAMSC	Steve Howard	T	2	270	1.3.2	Cryptographic migration should be mentioned here.	Add new last sentence: "Cryptographic migration to update algorithms or add algorithms (e.g., new secure hashing algorithms or Elliptic Curve Cryptography) are infrastructure wide and have a long period of change."	Declined. We already have several examples included.
ICAMSC-14	ICAMSC	Steve Howard	E	2	274	1.3.3	This section defines OCC: "...an optional On-Card Biometric comparison (OCC)..." and it is not used consistently throughout the document. And OCC is not a complete acronym.	Use the acronym consistently throughout the document. Recommend changing the acronym to "OCBC" to be consistent with the definition. Alternatively, use the more industry accepted match-on-card (MOC) for this acronym.	Solved by IBIA-1.
ICAMSC-15	ICAMSC	Steve Howard	T	3	287	1.3.5	There is no information on adoption/migration between versions of FIPS 201.	There needs to be a new special publication that specifies adoption practices for the incremental updates of FIPS 201. FIPS 201-2 should reference this document. Specifically, this new SP should cover sunrise and sunset processes, especially in relation to Sections 1.3.3 and Section 1.3.4.	Resolved by Cert-5.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-16	ICAMSC	Steve Howard	T	3	288	1.3.5	There must be a specific way to tell versions. This dictates how the physical infrastructure will migrate. Current language is "New version numbers may be assigned in [SP 800-73] depending on the nature of the change."	Proposed text: "New version numbers will, at a minimum, be assigned in [SP 800-73] specifically delineating non-backward compatible and deprecated or removed changes. In addition, [SP800-73] must provide a discovery mechanism that addresses changes defined in sections 1.3.1, 1.3.2, 1.3.3, and 1.3.4." This clarifies that 800-73 provides the technical version management and the means to detect changes that drive the physical infrastructure.	Resolved by Cert-6.
ICAMSC-17	ICAMSC	Jonathan Shu	T	3	288 - 291	1.3.5	The versions should be tied to specific releases of FIPS201 or appropriate NIST Special Publications. Also, text lacks specific requirements for when to introduce new version number. Specific text: "New version numbers **may** be assigned in [SP 800-73] **depending** on the nature of the change. For example, new mandatory features introduced in a revision of this standard, **may** necessitate a new PIV card application version number so that systems can quickly discover the new mandatory features. Optional features, on the other hand, **may** be discoverable by an on-card discovery mechanism."	Recommend specify types of changes that require new version number. I.e.: "New version numbers may be assigned in [SP 800-73] depending on the nature of the change. For example, all requirements changes in this standard or supporting specifications that require software changes to the card data model, or card edge or to the APIs (i.e. SP800-73 Part 3) shall be assigned a new version number. In addition, new mandatory features..."	Resolved by DoD-7.
ICAMSC-18	ICAMSC	Steve Howard	T	4	320-322	1.4	PIV Front-End Subsystem actually defines the credential, not a front-end system. Current text: "Section 4, PIV Front-End Subsystem, provides the requirements for the components of the PIV front-end subsystem. Specifically, this section defines requirements for the PIV Card, logical data elements, biometrics, cryptography, and card readers."	Proposed text: "Section 4, PIV Card Requirements, provides the requirements for the components of the PIV card. Specifically, this section defines requirements for the topology of the card, the electronic data model defining specific data elements including biometrics, cryptography. This section also introduces the concept of alternative form factors for future consideration in FIPS 201."	Declined. Section 4 represents requirements for Front-End Subsystem components as described in Figure 3-1.
ICAMSC-19	ICAMSC	Steve Howard	T	5	358-359	2.1	Current text does not address suitability independently from identity, causing confusion.	Proposed text: "Credentials are issued to individuals whose 1) true identity has been verified, 2) whose suitability has been confirmed, and 3) after a proper authority has authorized issuance of the credential;"	Declined: As noted in the Springer Memo, suitability determination is not required for all PIV Card applicants.
ICAMSC-20	ICAMSC	Jonathan Shu	T	5	358	2.1 First bullet (+) in second series	Remove "true" in referenced sentence, "Credentials are issued 1) to individuals whose true identity has been verified." The overall goal in long-standing Federal investigative processes and in FIPS 201 identity proofing is to authenticate the claimed identity of the applicant. To verify true identity adds the burden to conduct 1:N biometric matching against entire PIV population in the issuance and management system.	Recommend change text to "Credentials are issued 1) to individuals whose identity has been verified and 2) after a proper authority has authorized issuance of the credential;"	Resolved by deleting the word "true". Also in the definition of "identification" in Appendix E.1 (now Appendix C.1), remove the word "true".

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-21	ICAMSC	CPWG	T	6	377	2.2	Reference to Springer memo does not address subsequent updates or OPM direction	Recommend referencing the Springer memo with "including subsequent modifications per OPM guidance".	Resolved by replacing: "Federal departments and agencies shall use the Credentialing guidance as contained in a memorandum dated July 31, 2008, from Linda M. Springer, the Director of the Office of Personnel Management, to Heads of Departments and Agencies when determining whether to issue or revoke PIV Cards. [SPRINGER MEMO]" with: "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 departments and agencies shall also apply credentialing requirements specified in applicable OMB memoranda (e.g., OMB Memorandum M-05-24 [OMB0524])."
ICAMSC-22	ICAMSC	Jonathan Shu	T	6	386 - 389	2.3/Bullet 2	The second bullet in section 2.3 [on NACI, NCHC, etc.] should be cut and incorporated into section 2.2 on Credentialing Requirements. This is part of the "credentialing determination" process and can be linked to the identity proofing and registration via the chain of trust as described further in the section.	Recommend move 2nd bullet to 2.2 and change to: "The credentialing process shall begin with initiation of a NACI or equivalent. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI. Also, the FBI NCHC (fingerprint check) shall be completed before PIV issuance. Appendix B, Background Check Descriptions, provides further details on NACI."	Resolved by DoD-11.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-23	ICAMSC	Steve Howard	G	6-7	391-437	2.3	This text is very much improved over I-9, but primary and secondary identity documents change over time. FIPS 201 will not have an accurate list that lasts the full five year period.	Move identity proofing document requirements into a special publication.	The US Citizenship and Immigration Service's I-9 identity source document revision history indicates that the list of identity source document remain surprisingly stable, and that changes have tended to be related to verification of employment authorization rather than verification of identity. In order to help ensure the stability of the list of acceptable documents, the following three items will be deleted from the list of acceptable primary identify source documents: • Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa • In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form • Passport from the Federal States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the US and the FSM or RMI and a new item will be added that says: • A foreign passport
ICAMSC-24	ICAMSC	Steve Howard	T	6-7	391-437	2.3	No guidance is given to establish basic groundrules for comparison of (corroboration) and accuracy between source identity documents.	Ensure the new special publication identified in (comment 23) addresses guidance for comparison/corroboration between identity documents vs. the claimed identity.	Resolved by inserting the sentence in Section 2.7, 5th bullet: "The source documents shall be bound to that applicant."
ICAMSC-25	ICAMSC	CRFroehlich	E	6	393	2.3	Missing conjunction	Revise to read: "...nor cancelled, **and** shall be one..."	Resolved by NCE-8.
ICAMSC-26	ICAMSC	Steve Howard	T	6	394-410	2.3	This list does not include PIV or PIV-I cards.	Add PIV and PIV-I cards. If not for primary, at least for secondary. They are fully electronically verifiable and this is a significant advantage in the identity proofing process. If necessary, require Federal Common and FBCA CPs to be changed to reflect this ID proofing list, enabling this use.	Resolved by Cert-12.
ICAMSC-27	ICAMSC	Jonathan Shu	T	6	399 - 405	2.3	Question 1: What is the fundamental difference between Document 5 and 6? Question 2: Why was the DoD CAC specifically specified over other Federal PIV Cards? Need clarification on Bullet5: Construct a new Chain-of-Trust record shall be created in accordance with section 4.4.1 for the applicant.	Recommend clarify difference in accepting I94 vs. I94A with passport. Also, clarify if NIST was attempting to specify a DoD CAC population (Military).	Resolved by replacing the Common Access Card with the PIV Card on the list. Note: The chain-of-trust mechanism may be used to eliminate the need to repeat the complete registration and issuance process in these cases.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-28	ICAMSC	Steve Howard	E	6	401	2.3	"...containing an endorsement has not yet expired…"	"...containing an endorsement that has not yet expired…"	Resolved by ICAMSC-23.
ICAMSC-29	ICAMSC	CRFroehlich	G	7	411-413	2.3	Whereas the standard makes clear that the primary identity source document cannot be expired, no such statement exists to clearly indicate the status of the secondary identity source document.	Recommend specifying that the secondary identity source document must not be expired or cancelled.	Resolved by NCE-8.
ICAMSC-30	ICAMSC	Jonathan Shu	E	7	438	2.3/Bullet 5	For clarity, remove or modify the reference to "issuance" within 2.3 since this section is focused on identity proofing and registration (issuance is in 2.4). Also, other processes (credentialing, reissuance, renewal) apply in this case.	Recommend change 5th bullet to: "The PIV identity proofing and registration process, when combined with the remaining PIV processes, shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person."	Resolved by DoD-14.
ICAMSC-31	ICAMSC	Steve Howard	T	8	441	2.3	Forward reference to 4.4.1 should not be done. The chain-of-trust record is foundational to ID Proofing procedures. This section should specifically define establishment of the "chain-of-trust" record. 4.4.1 can then be used in the active authentication methods in concert with the other modes.	Establishing the "chain-of-trust" record as supported by enrollment must be defined in section 2.3. It is foundational to all lifecycle events that follow in this standard. Section 4.4.1 should deal authentication using the biometric. See following contribution (embedded object) to replace line 441.	Resolved by AMAG-6.
ICAMSC-32	ICAMSC	Jonathan Shu	G	7	442 - 444	2.3	The last paragraph on page 7 states, "The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head of the Federal department or agency." Requiring this level of senior level endorsement within a Federal department or agency is unnecessary and repetitive to the items C&A activity outlined in SP 800-79-1.	Strongly recommend changing to, "The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as outlined in SP800-79-1."	Resolved by DoD-15.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-33	ICAMSC	Jonathan Shu	T	8	445	2.3/ Last Paragraph pg. 8	Change last paragraph of this section to more specifically address the requirements for identity source documentation for citizens of foreign countries. The rationale is that the current language indicates that the requirements listed "also apply to citizens of foreign countries." However, it only goes on to state that a registration and approval process must be established – the paragraph does not address the fact that the requirement listed (specific list of source documents for primary and secondary documentation) cannot be applied to these individuals in all cases. Due to international agreements with host nations, citizens of foreign countries working for the Federal government may not have / be required to possess identity source documents from the I-9 list. Furthermore, the reference that the "identity proofing" requirement applies to foreign citizens, but a process for "registration and approval" must be established by other means is confusing. "Approval" should no longer be attributed to this section as it is addressed in the new 2.2 Credentialing Requirements section.	Strongly recommend change paragraph to: "The requirements for identity proofing and registration also apply to citizens of foreign countries who are working for the Federal government overseas. However, a process for identity proofing and registration must be established using a method approved by the U.S. Department of State's Bureau of Diplomatic Security, except for employees under the command of a U.S. area military commander."	Resolved by DoD-16.
ICAMSC-34	SKIPPED						NUMBER SKIPPED IN ORIGINAL COMMENTS		Noted.
ICAMSC-35	ICAMSC	Jonathan Shu	E	8	457 - 460	2.4/Bullet 3/Page 8	The bullet reiterates the investigative requirements – each times these requirements are mentioned the wording is slightly modified. Suggest changing the bullet to more directly tie the requirement to one place (Section 2.2 that was added for Credentialing Requirements)	Recommend change bullet to: "The process shall ensure that the credentialing requirements have been met in accordance with Section 2.2. The PIV Card shall be revoked if the results of the credentialing determination so justify." The second bullet of section 2.3 should also be moved to Section 2.2 so that the credentialing determination/investigative requirements are in one location.	Resolved by DoD-11.
ICAMSC-36	ICAMSC	Jonathan Shu	T	8	473	2.4	The statement "Cards that contain typographical defects, contain errors in optional fields, are not properly printed, or are not delivered to the cardholder are not considered PIV Issued Cards." Not sure this is a good idea from a security standpoint. If the card was intended to be issued as a PIV card, it should be treated as a PIV card. If there are errors on the card, it should be revoked, but all requirements connected with the management of the card and the revocation of it should be followed.	Recommend delete reference or clarify intent of addressing card with defects.	Resolved by Cert-18.
ICAMSC-37	ICAMSC	Steve Howard	T	8	474	2.4	"...are not properly printed, or are not delivered…"	"...are not properly printed, do not yet contain any PKI credentials, or are not delivered…"	Resolved by Cert-18.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-38	ICAMSC	Steve Howard	T	9	486-489	2.4.1	The reference to the employee name change section is not really appropriate. That processes establishes a legal name change with documentary evidence, then proceeds to re-issuance which requires the issuer to recover the previous card and destroy it. As such, an individual requiring a pseudonymous card can not retain their current PIV card.	Fully specify the requirements for ID Proofing and Issuance of a new PIV card under a pseudonym here. Specifically describe use of existing PIV as authentication for new pseudonymous PIV card. This may reference the re-issuance section, but this section must be clear that the original PIV card does not need to be recovered and destroyed. This concept aligns with the "derived PIV Card" paradigm"	Resolved by removing "for employee name changes" from the sentence "The issuance of a PIV Card using a pseudonym shall follow the procedures in PIV Card Issuance Requirements except that the employee must provide evidence satisfactory to the card issuer that the pseudonym is authorized by the employee's agency."
ICAMSC-39	ICAMSC	RJShanley	G	9	492-494	2.4.2	This language is too vague. It does not make clear what must be done to authenticate the card requestor or how the issuance process would differ from a new card request.	Add language to distinguish between a PIV card issuance during the 60-day grace period versus a new issuance.	Resolved by Cert-20.
ICAMSC-40	ICAMSC	Steve Howard	E	9	496	2.5	The reference to Appendix C is the last sentence of section 2.5 (line 645). It flows better and does not hide the reference in section 2.5.6 which is only about termination. Appendix C covers a lot more than termination.	Move the sentence at 645 to line 496 adding it as a second sentence: "A summary of PIV Card Issuance and PIV Card Maintenance requirements is provided in Appendix C."	Resolved by Cert-44.
ICAMSC-41	ICAMSC	Steve Howard	T	9	503	2.5	"...Backend Attribute Exchange…"	"…Federation Services (including Backend Attribute Exchange)…"	Resolved by Cert-21.
ICAMSC-42	ICAMSC	Steve Howard	T	9	506	2.5.1	This section is incorrectly named. Renewal is used very differently in PKI and smart card environments and this incorrectly re-defines renewal. PIV Card Renewal is actually renewing the PKI certificates at the 3 year mark, extending the life of that particular PIV card.	Change section to be: "PIV Card Routine Re-issuance Requirements" as you are not actually renewing the existing PIV Card. -or- pick a different word than "Renewal"	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.
ICAMSC-43	ICAMSC	Steve Howard	T	9	507	2.5.1	"Renewal is the process by which a valid PIV Card is replaced without…"	"Routine re-issuance is the process by which a PIV card that is reaching its expiration date (at the end of its 6 year lifetime) is replaced without…"	Resolved by Cert-23.
ICAMSC-44	ICAMSC	Jonathan Shu	T	9	507	2.5.1	Why specify a time limit for applying for a renewal card? There could be circumstances (individual is going to be deployed to a remote location) where it makes sense to renew a card more than 12 weeks prior to expiration.	Recommend just requiring that the current card has not expired and not specifying a time window.	Resolved by DHS-4.
ICAMSC-45	ICAMSC	Steve Howard	T	9	508-510	2.5.1	"The original PIV Card must be surrendered when requesting a renewal. The PIV Card is renewed only after a proper authority has authorized renewal of the credential."	Proposed text: "The original PIV Card must be surrendered during routine re-issuance. A proper authority must authorize routine re-issuance."	Resolved by Cert-23.
ICAMSC-46	ICAMSC	Steve Howard	T	9	511	2.5.1	"...current before renewing…"	"…current before routine re-issuance of…"	Resolved by Cert-23.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-47	ICAMSC	Steve Howard	T	9	517	2.5.1	"...apply for a renewal starting..."	"...apply for routine re-issuance starting..."	Resolved by Cert-23.
ICAMSC-48	ICAMSC	Steve Howard	T	9	519	2.5.1	"...renewal process..."	"...routine re-issuance process..."	Resolved by Cert-23.
ICAMSC-49	ICAMSC	Steve Howard	T	9	521	2.5.1	This is an open ended requirement with significant system level and privacy concerns. What is the PIV management infrastructure? It is undefined. "...and distribute the changed data within the PIV management infrastructure."	delete "and distribute the changed data within the PIV management infrastructure" from the sentence.	Delete the extra language at lines 521 and 500.
ICAMSC-50	ICAMSC	Steve Howard	T	10	525	2.5.1	Although the first sentence sets the minimum requirement, it is not operationally a good idea.	Add proposed sentence after the first sentence: "Issuers may elect to refresh the biometric data after reconnecting the applicant to their chain-of-trust record to improve operational effectiveness."	Resolved by Cert-30.
ICAMSC-51	ICAMSC	Steve Howard	T	10	528	2.5.1	Any certificate should not last longer than the card.	Recommend adding a requirement that any certificate should not last longer than the card.	Resolved by GSA-11.
ICAMSC-52	ICAMSC	Steve Howard	E	10	538	2.5.2	"(see Section 4.4.1)"	See comment 31 Amend to reference section 2.3 which establishes the chain-of-trust as a function of initial enrollment and issuance.	Resolved by AMAG-6.
ICAMSC-53	ICAMSC	Steve Howard	T	10	545-546	2.5.2	"The PIV Card itself is revoked. Any local databases that contain FASC-N values must be updated to reflect the change in status." is an open ended requirement. Revocation of a PIV Card is explicitly tied to the PIV Auth Cert. There is no other interoperable means of revoking a PIV Card.	Remove this item. The requirement is correctly stated in lines 547-556. All relying party systems are obligated to check the CRL/OCSP responders.	Declined. This text does not impose requirement on all relying system databases.
ICAMSC-54	ICAMSC	CPWG	T	10	547	2.5.2	Mandatory revocation of certificates that have not been or do not have the potential for the private key to be compromised only causes certificate revocation lists to grow and does not enhance security. And any time there is a potential for compromise of the key the certificate needs to be revoked. Stating that the certificate is revoked by placing the serial number on the CRL - really not a necessary statement - that is what the standard for CRLs calls for.	Replace current text about revocation request procedures with a reference to Common Policy CP.	See DHS-5. Accept to remove details on how to do revocation.
ICAMSC-55	ICAMSC	Steve Howard	T	10	557-558	2.5.2	"If the card cannot be collected, normal operational procedures shall be completed within 18 hours of notification." Normal operational procedures are not clear. Implies revocation.	Proposed text: "If the card cannot be collected, normal revocation procedures shall be completed within 18 hours of notification."	Resolved by Cert-36.
ICAMSC-56	ICAMSC	Steve Howard	T	10-11	564-566	2.5.2	Although this sentence sets the minimum requirement, it is not operationally a good idea.	Add proposed sentence after this sentence: "Issuers may elect to refresh the biometric data after reconnecting the applicant to their chain-of-trust record to improve operational effectiveness."	Resolved by Cert-30 and Cert-37.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-57	ICAMSC	Steve Howard	T	11	579	2.5.3	Re-Key is a special case of post issuance update	Add new last sentence: "Re-Key shall follow the requirements in section 2.5.4."	Resolved by Cert-38.
ICAMSC-58	ICAMSC	Jonathan Shu	G	11	595 - 956	2.5.4	This bullet states, "the PIV Card will communicate with no end point entity other than the PIV Card issuers during the remote post issuance update." DoD can envision the use of multiple Global PlatformTM domains on a single PIV in which the applications within the PIV domains would be managed by the PIV issuer and the application within a secondary domain may be managed directly by the owner of the line of business the domain is supporting. All of which would not weaken the overall security or integrity of the PIV credential.	Strongly recommend deleting the next to last bullet or adding text restricting this requirement by each security domain rather than the entire PIV credential.	Resolved by DoD-26.
ICAMSC-59	ICAMSC	Jonathan Shu	G	11	596 - 598	2.5.4	The last bullet within this section states, "If the PIV Card post issuance update begins, but fails for any reason, the PIV Card issuer shall immediately terminate the PIV Card as described in Section 2.5.6, and a diligent attempt shall be made to collect and destroy the PIV Card." This excerpt prescribes entirely too much about the potential implementations of post issuance capabilities by the PIV issuers. This statement has no context to the type of post issuance transaction that is attempting to be completed or were/what pieces of the processes fail or whether these other system technics in place to reprocess failed transactions.	Strongly recommend deleting this bullet. This level of implementation details are not standards, interoperability, or security related because not enough detail is know on a particular department or agency's implementation. These details must be left to the PIV issuer to determine.	Resolved by DoD-27.
ICAMSC-60	ICAMSC	Steve Howard	T	12	604-607	2.5.5	Need to separate cardholder changing their PIN when they know the old PIN, from issuer doing a reset on PIN block or PIN forgotten.	Proposed text: "The PIN on a PIV Card may need to be reset if the cardholder wants to change their PIN, if the cardholder has forgotten the PIN, or if PIN-based cardholder authentication has been disabled from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency (PIN blocked). If the cardholder knows the current PIN and the card and the card is not PIN blocked, the cardholder may reset their PIN upon presentation of the current PIN to the card. PIN resets may be performed by the card issuer. ..."	Resolved by removing PIN change from the text since PIN change is not the same as PIN Reset. Also, add the footnote: Cardholders may change their PINs anytime by providing the current PIN and the new PIN values.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-61	ICAMSC	Steve Howard	T	12	608-620	2.5.5	Issuer reset of verification data includes both PIN and biometric on card comparison reference data. There are not separate procedures for either of these as far as the issuer is concerned. Start a new paragraph and replace the text beginning with "PIN resets may be performed..." The proposed text for 1:1 match against the chain-of-trust is equivalent to the requirements in PIV-I for verification data (PIN) reset, maintaining the overall security of both PIV and PIV-I.	Proposed text: "The card issuer may reset verification data (including the PIN or on card biometric comparison data). Before reseting the PIV Card verification data, the card issuer shall reconnect the cardholder to the chain-of-trust record by performing a 1:1 match of the cardholder (see section 2.3). Upon successful match, the issuer may reset PIV Card verification data.[footnote 3] Departments and agencies may adopt more stringent procedures for verification data reset (including requiring in-person appearance or disallowing verification data reset, and requiring the termination of PIV Cards that have been locked); such procedures shall be formally documented by each department and agency."	Declined – The second paragraph in Section 2.5.5 (now Section 2.9.4) addresses the requirement for resetting biometric data. These requirements are different from PIN reset and should not be combined.
ICAMSC-62	ICAMSC	Steve Howard	T	12	621	before 2.5.6	There is no definition on what constitutes a revoked or expired PIV card. Per the workshop, the proposed language is offered to correct the hassles of "too many expiration dates".	Add the following section: 2.5.x PIV Card Revocation/Expiration Status A PIV Card is revoked if any of the following is true: - The PIV Authentication Certificate is revoked or PDVAL fails for the trust chain - The Card Authentication Certificate is revoked - Any certificate in the trust chain is revoked A PIV Card is expired if any of the following are true: - The PIV Authentication Certificate is expired - The Card Authentication Certificate is expired The expiration dates in the authentication certificates will always expire on or before the CHUID expiration date.	Resolved by Cert-41.
ICAMSC-63	ICAMSC	CRFroehlich	T	14	689-690	2.6	Security controls outlined in SP 800-53 and SP 800-53A have been augmented for PKI systems by the FPKIPA PKI Security Controls document. These sets of controls and evaluation methods should be applied to PKI CAs and associated systems, facilities, and personnel.	Recommend adding the following: "Security controls for PKI CAs and associated systems, facilities, and personnel are specified in Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53, Security Controls for PKI Systems; and, in Federal Public Key Infrastructure (FPKI) Security Controls Profile of Special Publication 800-53A, Assessment Guidance for Security Controls in PKI Systems. These security controls profiles should be used to establish and evaluate the security plans and controls of PKI systems."	Decline to reference specific SP 800-53 profiles, such as FPKI Security Controls Profile. By referencing SP 800-53, profiles are covered as well.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-64	ICAMSC	Steve Howard	T	15-19	698-826	3	This section is very clearly out of sync with the FICAM Segment Architecture and the FICAM Roadmap. Specifically, Figure 3-1 and the definitions that support it are no longer notionally correct.	This must be updated to harmonize with the FICAM Roadmap and Implementation Guidance v1.0, dated November 10, 2009, Section 2. This is the best federal document that defines ICAM architecture. This will clarify the separation of Identity Management and Credential Management from Access Management and reduce confusion in subsequent sections that merge these concepts using the current definitions in Section 3.	Resolved by Cert-47.
ICAMSC-65	ICAMSC	RJShanley	T	17	776	3.1.2	Unless you consider the actual PIV card a part of the PIV Card Issuance and Management Subsystem, some generation of key pairs takes place outside of the "key management component." In the case of the PIVAuth certificate, key pairs are generated on the card.	Recommend removing the text "...generation of key pairs,..."	Declined. The PIV Card issuance system's Key Management component is 'responsible' for key generation regardless of whether some keys are generated on-card or off-card.
ICAMSC-66	ICAMSC	Steve Howard	E	20	827	4	This section does not define a "Front-End Subsystem". It actually defines the PIV Card.	Rename the section. Proposed title: "PIV Card Requirements"	Resolved by Cert-54.
ICAMSC-67	ICAMSC	Steve Howard	T	20	828	4	Current text: "This section identifies the requirements for the components of the PIV front-end subsystem."	Proposed text: "This section identifies the requirements for the PIV Card."	Resolved by Cert-55.
ICAMSC-68	ICAMSC	Steve Howard	T	20	832	4	Current text: "Section 4.5 discusses card readers." This is the only section that is not directly related to the definition of the PIV Card. No new requirements are outlined (beyond conformance to ISO stds and SP800 series). It is very incomplete (wrt PACS in particular).	If Section 4.5 must be retained, proposed text: "Section 4.5 discusses card readers, providing minimum mandatory requirements for security and interoperability with the PIV Card."	Resolved by Cert-56.
ICAMSC-69	ICAMSC	Jonathan Shu	T	20	833 - 1122	4.1.1 thru 4.1.5	Card topology specifications are split between FIPS 201-2 and SP 800-104	Move all physical card and topology definitions (specifically sections 4.1.1 thru 4.1.5) into SP800-104 and make this a normative reference from FIPS 201-2.	Resolved by moving information from SP 800-104 to FIPS 201-2 and making Zones 15F and 18F mandatory. Also, withdraw SP 800-104.
ICAMSC-70	ICAMSC	Steve Howard	T	20	845	4.1	In accord with comment 69, make SP800-104 reference normative.	Add the following proposed text after "...[ISO14443].": "The specifications for the physical card and topology of a PIV Card are defined in [SP800-104]. These specifications include: - Printed Material - Tamper Proofing and Resistance - Physical Characteristics and Durability - Visual Card Topography - Color Representation"	Resolved by moving information from SP 800-104 to FIPS 201-2 and making Zones 15F and 18F mandatory. Also, withdraw SP 800-104.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-71	ICAMSC	Jonathan Shu	G	21	893 - 896	4.1.3	The bullet "Department and agencies shall ensure that the card meets the requirements of Section 508 of the Rehabilitation Act" is too broad for the purposes of this standard and should be deleted. It assumes that there are specific requirements in the act that can be attributed to PIV cards when, in fact, Section 508 is about the bigger issue of overall "access to and use of information and data" for individuals with disabilities. Attempting to outline a broad requirement specific to the physical topology of a PIV card does not take into account the case by case nature in which Section 508 compliance shall be addressed by each Agency.	Delete bullets on the broad requirement for 508 compliance. If a reference to 508 is still required delete bullet 5 and modify bullet 8 to read as follows: "Decals shall not be adhered to the card unless specifically required by an Agency to assist with compliance of Section 508 of the Rehabilitation Act. If a decal is used in this case (for example, an adhesive Braille letter) it shall be place in Zone 21F as defined in Section 4.1.4.3."	Resolved by DoD-32.
ICAMSC-72	ICAMSC	Steve Howard	T	21	943-951	4.1.4.1	Zone 2F attempts to define an authoritative name to be printed on the credential. The PKI credentials according to Federal PKI Common Policy Section 3.1 and FBCA Policy Section 3.1 actually define the name to ensure uniqueness across the entire Federal enterprise. Zone 2F and the corresponding entries in the printed information buffer are for human verification. These should not be confused with the authoritative names in the PKI credentials.	This needs to be ammended to define a Primary Printed Identifier and a Secondary Printed Identifier used for human visual verification in accordance with ICAO 9303. These identifiers shall be stored in the Printed Information Buffer defined by [SP800-73]. The Primary identifier is the last name (including generational identifier and punctuation). The Secondary identifier can be a common given name used on a daily basis (including nicknames and punctuation).	Decline to include generational identifier in primary identifier since we are following ICAO 9303 convention. Also, resolved by replacing lines 954-955 with the following: "Names in the Primary Identifier and the first name in the Secondary Identifier shall not be abbreviated. Other names and conventional prefixes and suffixes, which shall be included in the Secondary Identifier, may be abbreviated."
ICAMSC-73	ICAMSC	Jonathan Shu	T	24	973	4.1.4.2	4.1.4.2 Mandatory Items on the Back of the Card. The orientation of the back of the card has been changed from FIPS201-1 requirements. Hopefully the authors intended the engineering diagrams (which have been changed from the current FIPS 201 version) to indicate a view of the printing on the back of the card as seen through a transparent front. If that is not the case, these changes to the topography would have a significant impact to DoD's manufacturer's process. Such as: - What is shown would represent a departure from the ISO standard placement of the mag stripe. This custom change to the process for the PIV CAC would likely result in higher changeover and recurring manufacturing costs, and perhaps higher material costs. - Changing the position of the magnetic stripe from the right to the left side of the card (as shown in figure 4.7 on page 34) would require a manufacturing process change to deploy. The mag stripe is embedded in one of the bottom layers of the card when the card layers are fused together during production. Changing the orientation or the side on which the serial number of the card is laser engraved would likewise cause a change in the manufacturing process.	Strongly recommend that, If this was a engineering diagram indicating a view of the printing on the back as seen through a transparent front, the diagram must be marked according to the standards of that convention and should then be labeled as such. If the view intent is correct (same as in FIPS201-1), then DoD recommends clarifying the intent of the diagrams and making modifications to bring them back in line with the current FIPS 201 standard. Recommend moving these requirements to SP800-104.	Resolved by reverting back to FIPS 201-1, removing references to TSA, DOB, and Gender, adding 'B' to zone numbers. Removed reference to TSA as per resolution on comment number DHS-24.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-74	ICAMSC	Jonathan Shu	T	26	1023	4.1.4.3/ Zone 18F/page 26	The wording describes the Affiliation Color Code in "normative" language as opposed to being an optional feature.	Recommend change the Zone 18F wording to emphasize optional nature by added "If used, the affiliation color code "B" for Blue,..." etc.	Resolved by ICAMSC-69.
ICAMSC-75	ICAMSC	Steve Howard	T	38	1117, 1188, 1193	4.2, 4.2.1, 4.2.2	In concert with comment 76, these sections define the CHUID within the card data model. Renumber as part of section 4.1.	Renumber as follows: 4.2 becomes 4.1.2; 4.2.1 becomes 4.1.2.1; 4.2.2 becomes 4.1.2.2	Resolved by AMAG-6.
ICAMSC-76	ICAMSC	Steve Howard	T	36	1123	4.1.6	This begins the definition of the PIV Card Application and Data Model.	Rename the section and make it the same level as the Physical PIV Card Characteristics. Proposed: "4.2 PIV Card Application and Data Model"	Resolved by AMAG-6.
ICAMSC-77	ICAMSC	Steve Howard	T	36	1124	4.1.6	In concert with comment 76, "This section defines logical identity credentials and the requirements for use of these credentials." is not accurate.	Proposed text: "This section defines the PIV Card Application and Data Model. This provides the definition of PIV identity credentials and the requirements for the application that manages these credentials.	Resolved by AMAG-6.
ICAMSC-78	ICAMSC	Steve Howard	T	36	1125	4.1.6.1	In concert with comment 76 this section defines the PIV Card Data Model.	Rename section and make it level 3 in concert with comment 76 Proposed: "4.2.1 PIV Data Model"	Resolved by AMAG-6.
ICAMSC-79	ICAMSC	Steve Howard	T	36	1126-1128	4.1.6.1	In concert with comment 76 current text must be updated to reflect clarity in data model vs. logical credentials within the data model.	Proposed text: "...the PIV Data Model shall contain logical credentials composed of multiple data elements as specified in [SP800-73]. These data elements are for the purpose of verifying the cardholder's identity at graduated assurance levels. The mandatory data elements for a PIV Card are:"	Resolved by AMAG-6.
ICAMSC-80	ICAMSC	CRFroehlich	G/E	36-37	1132 + 1141	4.1.6.1	There appears to be a discrepancy between the requirements in lines 1132 and 1141; line 1132 specifies two iris images as mandatory data elements, whereas line 1141 specifies one or two iris images as optional data elements.	Clarify if two iris images or, one or two iris images are to be captured; and, are these data elements mandatory or optional.	Resolved by DoD-30. Collecting iris images is optional and it can be one or two iris images.
ICAMSC-81	ICAMSC	CPWG	T	37	1133	4.1.6.1	The proposed use of the CAK solely as an additional single factor authentication method is an inefficient use of card resources. In addition to interoperable PACS authentication, there is a need for encryption and privacy of the contactless interface and mutual authentication to establish trust with a terminal. Consideration should also be given to the increased key generation time during issuance and user experience with each additional key.	Strongly recommend to define the CAK and minimum additional keys and associated authentication mechanisms to support efficient PACS authentication (including mutual authentication) and secure contactless interface.	Resolved by DoD-36.
ICAMSC-82	ICAMSC	Steve Howard	T	37	1138	4.1.6.1	Current text limits to a single symmetric card auth key.	Proposed text: "Symmetric card authentication key(s) for…"	Resolved by Cert-85.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-83	ICAMSC	Steve Howard	T	37	1140	4.1.6.1	Facial image is optional. Most issuers are coding this on their cards today. Given card technology improvements, there is now sufficient space on the cards. Further, handheld verification devices need the photo for verification by guards. PIV-I makes the facial image mandatory. For interoperability, PIV should do the same.	Make the facial image mandatory.	Accept. In addition, replace "The electronic facial image may be used for the following purposes: + For generating the printed image on the card + For generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.1." with "The electronic facial image: + shall be stored on the PIV Card as described in Section 4.2.3.1; + shall be printed on the PIV Card according to Section 4.1.4.1; + may be used for generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.6; and + may be used for biometric authentication in operator-attended PIV issuance, reissuance, renewal, and verification data reset processes."
ICAMSC-84	ICAMSC	Steve Howard	T	37	1150	4.1.6.1	Reference to PIN only in "The PIN falls into the first category..."	Proposed text: "The PIN and on card biometric comparison data fall into the first category..."	Resolved by disposition of IGL-16.
ICAMSC-85	ICAMSC	Steve Howard	T	37-38	1152, 1158, 1169	4.1.7, 4.1.7.2, 4.1.7.2	These sections define application behavior and not the data model. Re-order in concert with comment 76.	Renumber as follows: 4.1.4 becomes 4.2.2; 4.1.7.1 becomes 4.2.2.2; 4.1.7.2 becomes 4.2.2.2	Resolved by AMAG-6.
ICAMSC-86	ICAMSC	Jonathan Shu	T	37	1153	4.1.7	The statement "The PIV Card shall be activated to perform privileged operations such as reading biometric information..." may not be applicable in the event that On-Card Biometric Comparison is implemented. This requires further clarification.	Recommend change statement to "The PIV Card shall be activated to perform privileged operations such as reading biometric information (in support of Off-Card Biometric Comparison)..."	Resolved by DoD-38.
ICAMSC-87	ICAMSC	Jonathan Shu	E	37	1159 -1162	4.1.7.1	Concerning the statement "PIV Cards shall implement user-based cardholder activation to allow privileged operations using PIV credentials held by the card. At a minimum, the PIV Card shall implement PIN-based cardholder activation in support of interoperability across departments and agencies. Other card activation mechanisms, only as specified in [SP 800-73], may be implemented and shall be discoverable.", is the expectation that the On-Card Biometric Comparison will enable privileged operations (such as releasing the private key)?	Consider specifying an example of another activation mechanisms, such as On-Card Biometric Comparison.	Resolved by DoD-39.
ICAMSC-88	ICAMSC	Steve Howard	T	37	1161	4.1.7.1	"Other card activation..." All modes of activation should be discoverable.	Proposed text: "Card activation..."	Declined. The PIN card activation method is the default method and should therefore activate the card without the need for discovery.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-89	ICAMSC	Jonathan Shu	T	38	1177	4.2	The statement that a CHUID should be treated as if it were a password doesn't make sense. The CHUID is significantly less secure than a password. A password is not supposed to be written down or recorded, but a CHUID can be obtained from anyone with a contactless reader and proximity to the card.	Recommend replace the current text with the following: The CHUID may be read and used by the relying systems, but it should be treated as an identifier only for purposes of authentication and retention. Because the CHUID is a static data object which can be read from the card, the CHUID is not considered resistant to cloning; it can be copied and used to gain access. It is strongly recommended that a complete CHUID should not be stored in relying systems.	Resolved by removing the third paragraph of Section 4.2 (now Section 4.2.1), Lines 1184-1187. Decline to indicate that PII data should be encrypted since it is already covered by FISMA.
ICAMSC-90	ICAMSC	Steve Howard	T	38	1178-1181	4.2	This should define explicitly what the mandatory and optional data elements are in the CHUID. The UUID must be mandatory for interoperability between PIV and PIV-I ecosystems. The details of formatting should be specified in [SP800-73], not in FIPS 201.	Replace the paragraph with this proposed text: "The PIV Card shall include the CHUID as specified in [SP800-73]. The following fields are mandatory in the CHUID: - FASC-N - GUID - Expiration Date - Issuer Asymmetric Signature"	see DoD-41.
ICAMSC-91	SKIPPED						NUMBER SKIPPED IN ORIGINAL COMMENTS		Noted.
ICAMSC-92	ICAMSC	Steve Howard	T	38	1184-1187	4.2	This paragraph is not correct. The CHUID is a static identifier. It is equivalent to a Userid. The CHUID is _not_ equivalent to a password. As it is an identifier, it should _never_ be used as an authenticator requiring the protection described in this paragraph.	Delete 1184 through 1187. There is no need for this paragraph.	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-93	ICAMSC	Steve Howard	T	38	1187	4.2	Missing a section on credential number requirements and how they are used within the PIV card to link objects together. See comment 168	Add a new section 4.2.1 (in concert with comment 75, this would be 4.1.2.1) as proposed: "The CHUID contains two credential identifiers that are unique to a given PIV card: FASC-N Identifier and a UUID. A subset of the FASC-N, the FASC-N Identifier, shall be unique to the PIV Card and is the concatenation of the Agency Code||System Code||Credential Number fields of the FASC-N. The UUID shall be unique to the PIV Card and is an RFC 4122 compliant Universally Unique Identifier. The UUID is stored in the GUID. The UUID and the FASC-N Identifier shall be used to link signed objects together within the PIV Card, as specified in [SP800-73] and [SP800-76]. The PIV FASC-N shall not be modified post issuance. The UUID shall not be modified post issuance."	See Cert-74.
ICAMSC-94	ICAMSC	Steve Howard	T	38	1188-1192	4.2.1	Per comment 72, this section is no longer necessary.	Delete this section.	See Cert-74.
ICAMSC-95	ICAMSC	Steve Howard	T	38-39	1199-1218	4.2.2	These details belong in SP 800-73 Part 1.	Move to SP 800-73 Part 1.	Resolved by Cert-75.
ICAMSC-96	ICAMSC	Steve Howard	T	39	1219-1223	4.2.2	In light of Advanced Persistant Threats, use of software certificates for content signing should no longer be allowed.	Delete references to id-fpki-common-devices which is a software level of assurance.	Replace 'id-fpki-common-devices' with 'id-fpki-common-devicesHardware.' See also NIST-16.
ICAMSC-97	ICAMSC	Steve Howard	T	39	1223	4.2.2	The CMS, PIV Content Signing Key, and Card Management Key do not have specific requirements that they must be protected as if they were CA keys and software. PIV-I specifically requires this.	Require protection of the CMS, PIV Content Signing Key and the Card Management master key in accord with CA level systems. Work with FPKIPA to update Common and FBCA CPs to reflect this change.	Resolved Cert-77.
ICAMSC-98	ICAMSC	CPWG	T	39	1223	4.2.2	Content Signing certificates should have a distinctive policy OID because they are inherently different from other device certs and the risks of compromise have higher impact	Recommend that the CMS and its keying material managed with equivalent protections to the CA keys	Resolved by ICAMSC-96.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-99	ICAMSC	CPWG	T	39	1223	4.2.2	A generic EKU should be specified in a Content Signing certificate because EKUs cannot be mapped and must be hard coded into applications, which runs counter to interoperability. See the IETF claimSigning Internet Draft (draft-king-pkix-claimsigning-extn-00) being discussed in the PKIX WG.	Recommend specifying the use of the claimSigning EKU being discussed in the PKIX WG (or specifying a similar mechanism)	Declined. We believe that there would be a few problems with changing FIPS 201 to require PIV Content Signer certificates to assert the claimSigning EKU rather than the id-PIV-content-signing EKU. First, it would be a non-backward compatible change that could negatively affect existing implementations that expect to find the current OID. Second, the claimSigning OID would not allow relying parties to distinguish between entities that are authorized to sign content on PIV Cards from entities that are merely authorized to sign claims of some form. Finally, there is no guarantee at this point that the IETF will ever assign an OID for the claimSigning EKU. It should be noted, however, that if a claimSigning EKU OID value is assigned and it is adopted for use in non-PIV content signer certificates, a requirement could be added (e.g., in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON]) for PIV Content Signer certificates to assert the claimSigning EKU in addition to the id-PIV-content-signing EKU, unless the document defining the claimSigning EKU OID value precludes asserting both EKU values in the same certificate.
ICAMSC-100	ICAMSC	Steve Howard	E	39	1225	4.3	This is card application specific.	In concert with comment 76, re-number to 4.2.3.	Resolved by AMAG-6.
ICAMSC-101	ICAMSC	Steve Howard	T	39	1231-1233	4.3	Once a secure channel is established, whether contact or contactless, all operations are allowed through the secure channel.	Allow PIN/Biometric verification, PKI operations, and read of all PIN protected services of a PIV Card through a secure channel (contact or contactless).	Resolved by AI-7.
ICAMSC-102	ICAMSC	Jonathan Shu	E	40	1244	4.3	The bullets on this page should be consistent about discussing PIN activation and interface availability.	A table would be helpful with columns: key name, key type (symmetric, asymmetric), activation (not required, unlock, per transaction), interface (contact, contactless, both).	Resolved by DoD-42.
ICAMSC-103	ICAMSC	Jonathan Shu	T	40	1245	4.3	Document states, "The PIV authentication key shall be an asymmetric private key that is accessible from the contact interface…" The private key itself is not accessible.	Recommend change text to "The PIV authentication key shall be an asymmetric private key that supports card authentication for an interoperable environment via challenges and signed responses via the contact interface."	Resolved by DoD-43.
ICAMSC-104	ICAMSC	Steve Howard	T	40	1246	4.3	The PIV Auth cert authenticates the cardholder, not just the card. Current text "…and supports card authentication for…"	Proposed text: "…and supports authentication of the card and cardholder for…"	Resolved by DoD-43.
ICAMSC-105	ICAMSC	Jonathan Shu	T	40	1248	4.3	Document states, "The asymmetric card authentication key shall be a private key that is accessible over the contactless and contact interface and supports card authentication for an interoperable environment." The private key itself is not accessible.	Recommend change text to "The asymmetric card authentication key shall be an asymmetric private key that supports card authentication for an interoperable environment via challenges and signed responses via the contactless and contact interfaces."	Resolved by DoD-44.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-106	ICAMSC	Steve Howard	T	40	1250	4.3	This key should be allowed to establish secure messaging, not just card authentication.	Add a new second sentence: "This key may also be used with secure messaging protocols as specified in [SP 800-73]."	Resolved by Cert-80.
ICAMSC-107	ICAMSC	Jonathan Shu	T	40	1252	4.3	The symmetric key can be used through either interface (contact or contactless). If so, it should be stated.	Recommend adding the following text "The symmetric card authentication key can be used via either the contactless or contact interface."	Resolved by DoD-45.
ICAMSC-108	ICAMSC	Jonathan Shu	T	40	1253	4.3	State that the digital signature key is used only with the contact interface	Recommend adding the following text "The digital signature key is an asymmetric private key supporting document signing via the contact interface …"	Resolved by DoD-46.
ICAMSC-109	ICAMSC	Jonathan Shu	T	40	1255	4.3	State that the key management key is used only with the contact interface.	Recommend adding the following text "The key management key is an asymmetric private key supporting key establishment and transport via the contact interface, and it is optional.	Resolved by DoD-47.
ICAMSC-110	ICAMSC	Steve Howard	T	40	1260-1261	4.3	Unless these keys are mandatory, they are not interoperable across the federal enterprise.	Add second sentence: "These key(s) may not be interoperable across the federal enterprise." Consider making a secure messaging protocol mandatory for general use on the card over any interface.	Declined as per Cert-81. Declined - all new feature are added as optional -- see change management section.
ICAMSC-111	ICAMSC	Jonathan Shu	T	41	1276	4.3	Change the following text: "Issued PIV Authentication certificates shall also include a PIV NACI indicator extension, until such time that OMB approves a government-wide operational system for distribution of Background Investigation status information (see Section 2.5). OMB is working on OMB a government-wide operational system for distribution of Background Investigation status information (see Section 2.5). When such a system becomes operational, relying parties will be required to check that system as part of access control decisions." Rationale specified in proposed **change.**	Strongly recommend change text to "Since agencies are not updating the NACI indicator in certificates after a person's investigation has been completed, the NACI indicator is now optional and deprecated."	After discussions with OMB, the NACI indicator requirements will remain as previously specified in FIPS 201-1 and in M-05-24. The second draft of FIPS 201-2 will be changed accordingly to reflect this. See also DoD-48.
ICAMSC-112	ICAMSC	Steve Howard	E	41	1281	4.3	"…infrastructure for PIV authentication…"	…infrastructure for the PIV authentication…	Accept.
ICAMSC-113	ICAMSC	Steve Howard	T	41	1293-1298	4.3	If using protocols like Opacity or MR PIV, symmetric keys are established without issuer involvement.	State that there may be more than one symmetric or asymmetric card authentication key and that it may be imported by the issuer or as part of a secure messaging protocol.	Resolved by Cert-85.
ICAMSC-114	ICAMSC	Steve Howard	T	41	1296	4.3	"The card authentication key shall be available…"	"Protocols using symmetric card authentication key(s) shall be available…"	Resolved by Cert-86.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-115	ICAMSC	Steve Howard	E	42	1316	4.4	This is card application specific.	In concert with comment 76 re-number to 4.2.4.	Resolved by AMAG-6.
ICAMSC-116	ICAMSC	CRFroehlich	G/E	42	1323 + 1326	4.4	There appears to be a discrepancy between the requirements in lines 1323 and 1326; line 1323 specifies two iris images as mandatory data elements, whereas line 1326 specifies one or two iris images as optional data elements.	Clarify if two iris images or, one or two iris images are to be captured; and, are these data elements mandatory or optional. [*NOTE: This confusion occurs in multiple places throughout the document.*]	Resolved by NCE-37.
ICAMSC-117	ICAMSC	Steve Howard	T	42	1331	4.4	"...the contact interface..." should allow secure messaging access for contactless biometric operations in PACS. This applies equally between on card comparison and off card comparison of the two electronic fingerprints.	Proposed text: "The PIV biometric data, except for on-card biometric comparison data, stored on the card shall be only accessible through the contact interface and after the presentation of a valid PIN. Contactless access of the PIV biometric data is allowed through a secure messaging protocol after presentation of a valid PIN. After a secure messaging session has been established, cardholder verification using on-card biometric comparison data may be available through the contact and the contactless interface of the PIV Card to support card activation (section 4.1.7.1) and cardholder authentication (section 6.2.5). The PIV Card shall not permit exportation of the on-card biometric comparison data. If implemented, PIV on-card biometric comparison data shall be implemented and used in accordance with [SP 800-73] and [SP 800-76]."	Resolved by AI-7.
ICAMSC-118	ICAMSC	Steve Howard	T	42-44	1338-1414	4.4.1	The definition of biometric chain-of-trust is critical to Section 2.3 and should be defined there.	See comment 31 Delete section 4.4.1 as it has moved into section 2.3 as part of ID Proofing and Registration Requirements	Resolved by AMAG-6.
ICAMSC-119	ICAMSC	R. L. Doty	T	43	1378	4.4.1	Despite the fact that 10 fingerprints may be able to be captured, they may be of such poor quality that they are useless for identification. This could be due to issues such as seriously burned individuals, whose fingerprints are not easily read.	Suggest that the language be modified to include an option to capture iris images where the fingerprints can be captured, but are inadequate. Recommend rewording to read: "...is not possible or results in poor quality, two iris images..." Note: The capture of iris should be an alternative, but not mandated at this time due to expense of implementation and the perceived lack of maturity of the technology.	Resolved by removing the requirement to collect iris - see DOJ-10 and GSA-21. The handling of poor quality fingerprints is addressed in NCE-37.
ICAMSC-120	ICAMSC	CRFroehlich	G/E/T	44	1408-1414	4.4.1	This subparagraph is confusing, and may be misplaced in the document given that (A) it appears to discuss the use rather than the collection of biometrics. (B) fingerprint templates without identifying a standard for those templates in the document and which may differ widely; (C) only fingerprints are addressed while iris images--permitted earlier in this section--are not addressed	Recommend rewording this entire sub-paragraph to: (A) eliminate the apparent link to biometric use rather than collection; (B) eliminate or specify "fingerprint templates"; and, (C) address all acceptable biometrics rather than just fingerprints	Resolved as follows: 1. The text will be moved and reworded in Section 6. 2. The section titles will be renumbered by AMAG-6, which separates biometric collection from use. 3. The standards governing fingerprint templates are specified in SP 800-76.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-121	ICAMSC	Steve Howard	T	44	1421	4.4.2	"The format for CBEFF_HEADER is specified in [SP 800-76]."	"The format for the biometric data, the CBEFF_HEADER and the CBEFF_SIGNATURE_BLOCK are specified in [SP 800-76]."	Accept, per Cert-91.
ICAMSC-122	ICAMSC	Steve Howard	T	44-45	1422-1453	4.4.2	This defines the details of the signature block.	Move text in lines 1422-1453 entirely into [SP800-76].	Accept, per Cert-91/92.
ICAMSC-123	ICAMSC	Steve Howard	T	45-46	1454-1458	4.4.2	Advanced Persistent Threats must be taken into account. id-fpki-common-devices software certificates should not be allowed.	Delete references to id-fpki-common-devices which is a software level of assurance.	Resolved by Cert-96.
ICAMSC-124	ICAMSC	Steve Howard	E	46	1459-1464	4.4.3	This text is duplicative. Specifications for biometric data are always called out in [SP800-76]	Delete this section.	Accept.
ICAMSC-125	ICAMSC	Steve Howard	E	46	1465	4.5	This is over and above card data model and card application.	In concert with 84, renumber this section as 4.3	Resolved by AMAG-6.
ICAMSC-126	ICAMSC	Steve Howard	T	46	1468-1483	4.5.1, 4.5.2	4.5.1 and 4.5.2 do not provide any new requirements that are not already defined in [SP800-73] or [SP800-96].	Delete these sections.	Declined. FIPS 201 is the authoritative document that establishes the high-level requirements. The technical details implementing FIPS 201 requirements are provided in Sps.
ICAMSC-127	ICAMSC	Steve Howard	T	46-47	1484-1494	4.5.3	Application of ISO24727 is much broader than just the reader. In particular, the interfaces are more at a system level protecting the application from variations in card profiles. Commerce should look at 24727, GICS and propose profiles for both to minimize change throughout the Federal enterprise. This is out of place in the FIPS 201, which defines the PIV Card, its content, and its issuance requirements.	Delete this section. But certainly do proceed with the work effort to leverage 24727. There is no unique requirement for a source of authority to proceed with that endeavor. It is not specific to PIV. It also covers PIV-I and nonPIV/PIV-I credentials.	Declined: This section has been added to allow possible future inclusion of an ISO/IEC 24727 profile that enables middleware a degree of independence from credential interfaces and vice versa.
ICAMSC-128	ICAMSC	CRFroehlich	G/E	46-47	1485-1494	4.5.3	The last sentence of this paragraph contradicts the characterization in the preceding sentences by implying that what was to be "...an optional profile of ISO/IEC 24727..." will become mandatory at some future, unspecified date.	Recommend that this apparent contradiction be resolved; either this profile will be optional or mandatory.	Resolved by modifying the sentence on line 1492 to: Specifications of the profile will become effective, as an optional means to implement PIV System readers and middleware, when OMB determines that the profile specifications are complete and ready for deployment.
ICAMSC-129	ICAMSC	Steve Howard	E	47	1495	4.5.4	renumber this section in concert with 102	Renumber to 4.3.1	Resolved by AMAG-6.
ICAMSC-130	ICAMSC	Steve Howard	T	47	1495	4.5.4	This section applies to any card activation data, not just PIN.	Rename "Card Activation Device Requirements"	Resolved by Cert-98.
ICAMSC-131	ICAMSC	Jonathan Shu	T	47	1500	4.5.4	The statement "If the PIN input device is not integrated with the reader, the PIN shall be transmitted securely and directly to the PIV Card for card activation." does not contain guidance for desktop computers.	Recommend adding, "Devices used with a PIV Card and card reader shall undergo frequent automatic integrity scans, to include virus and other malware checks, to prevent capture and disclosure of the PIN."	Resolved by adding the following text to Section 4.4.4, Card Activation Device Requirements. "Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document." Add reference to SP 800-53.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-132	ICAMSC	Jonathan Shu	T	48	1527	5.2.1	Reference is made to [PROF] for the certificate profiles. It is unclear why an LDAP URL is required for the Card authentication profile whereas legacy PKIs were exempted from LDAP for the PIV Authentication certificate. LDAP is blocked within DoD and cannot readily take advantage of caching.	Recommend change text to "…conform to Worksheet 8: …in [PROF]; except that the requirement for LDAP URLs is deprecated."	Since Worksheet 8 in the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF] was specifically written to specify the requirements for the Card Authentication Certificate, we believe this comment is best address by modifying [PROF] rather than by changing the referenced line in FIPS 201-2.
ICAMSC-133	ICAMSC	CPWG	T	49	1541	5.3	"PIV private keys shall issue CRLs every 18 hours, at a minimum." 18 hours is not conducive to issuing at a fixed time daily.	Recommend referencing the Common Policy for CRL issuance and validity periods.	Resolved by DHS-8.
ICAMSC-134	ICAMSC	Jonathan Shu	T	49	1545 - 1549	5.4	Change the following paragraph: "PIV Authentication Certificates and Card Authentication Certificates issued by legacy PKIs shall meet the requirements specified in Section 5.2.1. Departments and agencies may assert department or agency-specific policy OIDs in PIV Authentication Certificates and Card Authentication Certificates in addition to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively." The rationale is as follows: During the SHA-2 transition and use of new policy OID, we have discovered that asserting policy OID from one domain removes the flexibility for both sides of cross certified domain. It is desirable to map the policies to provide requisite security and flexibility to cross-certified domains. For the policy assertions to work securely, the applications should process policies and policy mapping appropriately and not just pick the policy in the end certificate. Thus, mapping to appropriate policies (as opposed to direct assertion) will provide requisite security while maintaining flexibility.	Recommend change to: "PIV Authentication Certificates and Card Authentication Certificates issued by legacy PKIs shall meet the requirements specified in Section 5.2.1. Departments and agencies may assert department or agency-specific policy OIDs in PIV Authentication Certificates and Card Authentication Certificates and map these OIDs to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively or may directly assert the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively."	Resolved by DoD-58.
ICAMSC-135	ICAMSC	RJShanle y	G	49	1566	5.5	HTTP should also be called out as a mandatory source for CRLs.	Add HTTP as a mandatory CDP	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-136	ICAMSC	Jonathan Shu	T	49	1566	5.5	Document states, "CAs that issue authentication certificates shall maintain an LDAP directory server that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it." LDAP is blocked by DoD and does not readily support caching. Recommend making HTTP 1.1 the standard and deprecating LDAP.	Recommend that CAs that issue authentication certificates shall maintain a repository that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it. The repository shall make CRLs available via HTTP 1.1 and may optionally support LDAP during a transition period. LDAP is deprecated.	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.
ICAMSC-137	ICAMSC	CRFroehlich	G/T/E	49-50	1573-1581	5.5.1	This section is unclear as to whether or not this requirement applies to legacy PKIs; and, is not addressed in Section 5.4.	Recommend addressing requirements for legacy PKIs specifically wherever appropriate throughout the document.	Resolved by replacing “PIV Authentication Certificates and Card Authentication Certificates issued by legacy PKIs shall meet the requirements specified in Section 5.2.1.” with “Legacy PKIs that issue PIV Authentication certificates and Card Authentication certificates shall meet the requirements specified in Sections 5.2.1, 5.3, 5.5, 5.5.1, and 5.5.2, with respect to the PIV Authentication certificates and Card Authentication certificates that they issue.”
ICAMSC-138	ICAMSC	Jonathan Shu	T	49	1573	5.5.1	The document says, "This standard requires distribution of CA certificates and CRLs using LDAP and Hypertext Transport Protocol (HTTP)." LDAP should be deprecated.	Recommend changing text to "This standard requires distribution of CA certificates and CRLs using Hypertext Transport Protocol (HTTP). LDAP is permitted as well, but is deprecated."	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.
ICAMSC-139	ICAMSC	Jonathan Shu	G	50	1576 - 1581	5.5.1	This section appears to infer any x.509 public key infrastructure (asymmetric cryptography) certificate that contains the FASCN or some representation of the FASCN cannot be make publically available. This requirement makes no sense when trying to use PKI as intended and supporting interoperability/cross recognition of PKI certificates amongst federal issuers. Public certificates must be public. It is not clear what the concern may be with the FASCN as part of the CHUID being within a public certificate, when the CHUID is a free read on contact and contactless interfaces of the PIV.	Strongly recommend deleting this requirement. Treating the FASCN as a secret instead of an identifier is an intrinsic risk to Relying Parties.	Resolved by DoD-61.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-140	ICAMSC	Steve Howard	T	52-58	1637-1815	6.2	These methods of authentication and their assurance levels are outdated in regards to PACS. The operational sequences are optimized differently than on PCs. Leveraging the PAK or CAK certificate in place of reading the CHUID is often done and just as valid.	Update these authentication scenarios and their assurance levels in accord with the Federated PACS Guidance document from the FICAM AWG.	Resolved by Cert-101.
ICAMSC-141	ICAMSC	Steve Howard	T	52	1643	6.2	Current text: "...is strengthened through the use of a…"	Proposed text: "...is requires the use of a…" CPWG also suggests moving this type of detail out of FIPS-201 to SP800-53	Resolved by deleting the first two sentences of the paragraph.
ICAMSC-142	SKIPPED						NUMBER SKIPPED IN ORIGINAL COMMENTS		Noted.
ICAMSC-143	ICAMSC	RJShanley	G	53	1662	6.2.1	This precedes a subset of optional components.	Update text to indicate the list is not inclusive.	Resolved by revising the sentence as follows: "The PIV Card may also bear optional components, some of which are:"
ICAMSC-144	ICAMSC	Steve Howard	T	53-54	1685-1686	6.2.1	These statements are no longer true. It is very easy to print up a new card that looks valid. They certainly will look unaltered during visual inspection.	Delete 1685-1686.	Declined. The text says low resistance to tampering and forgery, which is consistent with the comment that it is very easy to print up a new card that looks valid.
ICAMSC-145	ICAMSC	Steve Howard	T	54	1694	6.2.2	See comment 62.	Replace with: "Expiration and Revocation shall be checked in accord with section [???]."	Declined. We accept that some Authentication mechanisms do not protect against revoked cards. Specifically update those authentication mechanisms to highlight the vulnerability.
ICAMSC-146	ICAMSC	Steve Howard	T	55	1722	6.2.3.1	See comment 62.	Replace with: "Expiration and Revocation shall be checked in accord with section [???]."	Declined. We accept that some Authentication mechanisms do not protect against revoked cards. Specifically update those authentication mechanisms to highlight the vulnerability.
ICAMSC-147	ICAMSC	RJShanley	G	55	1723	6.2.3.1	A PIN should not be required if possession of the card and a live biometric sample are provided at the time of authentication. In ALL instances, the optional feature of biometric (fingerprint) activation of the card, without PIN entry, is uniformly referred to as "on-card biometric comparison." While accurate when standing alone, when intermixed with references to the PIV biometric, it consistently implies that matching of the PIV biometric (after PIN entry) is always OFF card.	If this is the requirement for both biometrics, then it effectively requires three-factor authentication; but, if this inadvertently precludes a valid possibility for on-card matching of the mandatory PIV biometric, then phrasing and section headers should be reviewed and amended as appropriate. In either case, the standard should allow PIV card activation with live presentation of biometric as an alternative to a PIN.	Declined. BIO specifically describes off-card matching authentication mechanisms. On-card biometric comparison is addressed in Section 6.2.5 (now Section 6.2.2). Changed the title of Section 6.2.3 (now Section 6.2.1) to "Authentication Using Off-Card Biometric Comparison" as per comment ICAMSC-148.
ICAMSC-148	ICAMSC	CPWG	E	57	1792-1801	6.2.3	The guidance regarding PIV authentication using on-card biometrics is currently in section 6.2.5, but would seem to be more appropriate in section 6.2.3.	Recommend moving section 6.2.5 to be the first subsection in section in 6.2.3.	Resolved by changing the title of Section 6.2.3 (now Section 6.2.1) to "Authentication Using Off-Card Biometric Comparison" and moving Section 6.2.5 to Section 6.2.2.
ICAMSC-149	ICAMSC	Jonathan Shu	E	55	1734	6.2.3.2	Since the attended authentication of PIV Biometric is nearly the same as unattended, the difference should be highlighted rather than repeat the entire set of steps.	Recommend change text to "The attended authentication of PIV Biometric is nearly the same as unattended authentication, except that the attendant observes submission of the biometric sample, thus increasing protection against spoofing."	Resolved by removing the steps 1-9 (lines 1735-1749) and modifying the sentence as follows. "This authentication mechanism is the same as the unattended biometrics (BIO) authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-150	ICAMSC	Steve Howard	T	55	1737	6.2.3.2	See comment 62.	Replace with: "Expiration and Revocation shall be checked in accord with section [???]."	Declined. We accept that some Authentication mechanisms do not protect against revoked cards. Specifically update those authentication mechanisms to highlight the vulnerability.
ICAMSC-151	ICAMSC	RJShanley	E	56	1757	6.2.4	"collect" should be "collected"	Change "collect" to "collected"	The sentence containing this typographical error has been deleted.
ICAMSC-152	ICAMSC	Jonathan Shu	T	56	1760	6.2.4.1	The "Authentication with the PIV authentication certificate credential (PKI-AUTH)" section only mentions the use of a PIN to activate the card. How will this section allow for other activation mechanisms that are expected to be specified in [SP 800-73]?	Recommend including a hook to reference other activation mechanisms (e.g., On-Card Biometric Comparison) as specified in [SP 800-73].	Resolved by the following changes: - Combine steps 2 and 3. - Add a sentence – If implemented, other card activation mechanisms, as specified in [SP 800-73], may be used to activate the card. - Change the characteristics to - Strong resistance to use of unaltered card by non-owner since card activation is required.
ICAMSC-153	ICAMSC	Steve Howard	T	57	1795	6.2.5	Current text: "...verification. A live-scan biometric…" does not mitigate YES machine behavior.	Proposed text: "...verification. A secure session is established with the card. A live-scan biometric…" May need more detail here based on secure session protocol in [SP800-73].	Declined. Section 6.2.5 (now Section 6.2.2) states the response includes information that allows the card to be authenticated. Details of how this will be accomplished will be provided in SP 800-73.
ICAMSC-154	ICAMSC	Steve Howard	E	57	1800	6.2.5	"...biometric, alf agencies…"	"...biometric, if agencies…"	Accept.
ICAMSC-155	ICAMSC	RJShanley	E	57	1800-1801	6.2.5	There are a couple of typos in this sentence: "As with authentication using PIV biometric, alf agencies choose to implement On-card biometric comparison it shall be implemented as defined in [SP 800-73] and [SP 800-76]."	Change to: "As with authentication using PIV biometric, if agencies choose to implement on-card biometric comparison, it shall be implemented as defined in [SP 800-73] and [SP 800-76].	Accept.
ICAMSC-156	ICAMSC	Steve Howard	T	57	1809	6.2.6	See comment 62.	Replace with: "Expiration and Revocation shall be checked in accord with section [???]."	Declined. We accept that some Authentication mechanisms do not protect against revoked cards. Specifically update those authentication mechanisms to highlight the vulnerability.
ICAMSC-157	ICAMSC	Jonathan Shu	T	57	1811	6.2.6	Document says, "The card responds to the previously issued challenge by signing it using the symmetric card authentication key." Symmetric keys are not capable of signature.	Recommend change text to "The card responds to the previously issued challenge by encrypting the challenge using the symmetric card authentication key."	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-158	ICAMSC	Jonathan Shu	G	58	1820-1823	6.3	The statement "Two or more complementing identity authentication mechanism may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder. For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in cardholder identity." is somewhat misleading, when considered in the context of OMB-04-04 E-Authentication Levels described earlier in the section. If PKI-AUTH already provides "VERY HIGH Confidence" for Physical and Logical (both Local and Remote) Access by itself, what sort of credit is given towards the additional application of BIO (i.e., what is the incentive to perform the extra step)? Requires clarification.	Recommend clarify reason or incentive to perform the extra BIO step, given that PKI-AUTH provides "VERY HIGH Confidence".	Declined. We would like to maintain consistency with SP 800-63, which requires two factors of authentication for VERY HIGH assurance level. We note that Table 6-2 defines the minimum requirement for each assurance level. FIPS 201-2 Section 6.3, introductory paragraph already says "Two or more complementing authentication mechanisms may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder. For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in cardholder identity."
ICAMSC-159	ICAMSC	Steve Howard	T	58	1839-1845	6.3.1	This table is outdated and inaccurate.	Replace with the table extracted from the FICAM AWG Federated PACS Guidance document - see embedded object below.	Resolved by downgrading CHUID and VIS and by adding LITTLE or NO ASSURANCE level to Tables 6-2 and 6-3.
ICAMSC-160	ICAMSC		T	59	1855	Table 6-3	Why is BIO-A included for logical access; according to 6.2.3.2, BIO-A stands for Attended Authentication of PIV Biometric.	Recommend deleting BIO-A from Table 6-3.	Declined. While it may be unlikely to use this authentication mechanism in attended local workstation environment, it is not impossible.
ICAMSC-161	ICAMSC	Jonathan Shu	E	61	1915	A.4	There may be some confusion with the phrase, "...validated to FIPS 140 with an overall Security Level 2 (or higher). [FIPS140-2]" Some may think the "-2" is the level.	Recommend change text to "...validated to [FIPS 140] or later certified to an overall security level of 2 (or higher). "	Accept - Also make similar changes throughout the document for consistency.
ICAMSC-162	ICAMSC	Steve Howard	T	61	1927	A.5	It is anticipated that more product families will get tested, especially in light of PACS testing program growth. Current text: "The product families include…"	Proposed text: "The product families currently include…"	Accept.
ICAMSC-163	ICAMSC	Jonathan Shu	T	62	1934-1946	Appendix B	Appendix B: Description of the NACI: Recommends this detail be removed. The NACI will be replaced by Tier 1 when the new Federal Investigative Standards are promulgated. Suggest FIPS 201-2 reflect	Recommend change text to "NACI or equivalent investigation as determined by Federal Investigative Standards" and leave out details.	Resolved by deleting Appendix B per OPM-6.
ICAMSC-164	ICAMSC	Jonathan Shu	E	64	1955	D.1	Missing useful information.	Recommend expanding the table to include the Policy OIDs as well so that all OIDs could be found in one location.	Declined. We are afraid that people start to use them without knowing what they mean.
ICAMSC-165	ICAMSC	Steve Howard	E	77	2355	Appendix G	"This version represents 5 year review of FISP 201…"	"This version represents 5 year review of FIPS 201…"	Accept.
ICAMSC-166	ICAMSC	Steve Howard	E	77	2355	Appendix G	"...received from agencies. Following is…"	"...received from agencies. Following are…"	Resolved by Cert-118.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
ICAMSC-167	ICAMSC	Jonathan Shu	T	N/A	General	New	FIPS 201 currently does not permit non-PIV data objects on PIV cards. This creates problems for issuers who require secure storage of organization specific, identity related data. Hosting non-PIV data on a second card application creates compatibility problems with middleware and security issues with PIN management and binding non-PIV identity data with the identity credentials on the PIV card. The only viable solution to this problem is to allow the creation of agency specific data objects within their own name space on PIV cards accessible through the standard PIV API.	Strongly recommend specify the use of the of the inter-agency namespaces as outlined in NISTR 7284 to permit issuers to create organization specific data objects on PIV cards	Resolved by DoD-1.
ICAMSC-168	ICAMSC	CPWG	G	0	0	General	FIPS 201-2 does not specify use of UUID.	FIPS 201-2 must address UUID per the definitions in SP 800-73. Note: DoD would like to see the UUID remain optional, but all other input requested as a mandatory implementation with adequate timelines for implementation.	See DoD-41.
ICAMSC-169	ICAMSC	ALHerto	E	General			Throughout the document, there is confusion regarding biometrics off-card versus on-card in section headers, many of which are not clearly resolved in the section text.	Recommend clearly specifying in section headers if the text relates to off-card or on-card biometrics.	Accept, for example in the in newly numbered Section 6, to explicitly mention "on-card".
ICAMSC-170	ICAMSC	Jason Ramsey PGS	T					Require crypto signature on biometric security object.	Section 4.4.2 (now Section 4.2.3.2) already requires a digital signature on all biometrics.
IDTP-1	IDTP	Dave Auman	G			General	PIN-to-PACS might be considered within scope of FIPS 201 if the PACS PIN is established as a proxy for the card PIN during a PACS Registration event where the card PIN (identity) is verified. In this case FIPS 201 might specify required security, entropy and chain of trust for this type of operation.		Resolved by SCA-54.
IDTP-2	IDTP	Dave Auman	G			General	APL Reader Type categories seem to be treating reader FEATURES as reader TYPES. Separately testing reader features within independent reader type categories does not assure that features work correctly when combined (i.e. PIV AUTH conformance + Biometric Conformance is not equal to PIVAUTH + BIOMETRIC Conformance).	Should consider creating SP 800 series defining unambiguous access control requirements and use cases following the lead of ICAM activities. ICAM work is good in this area but normative technical specs are needed to support a better conformity assessment regime.	Out-of-Scope.
IDTP-3	IDTP	GL	G	2	270	1.3.2	The text says: ".... 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." Using the Partial Select of ISO in terminals would solve the issue	In terminals, use the Select AID APDU command with only 9 bytes of the AID (partial Select). **See detailed explanations in the IDTP detailed comments word document.**	Noted.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IDTP-4	IDTP	GL	E	5	374	2.1	"An issued credential is not modified, duplicated, or forged". Credentials can be updated by the issuers (e.g. update of the PIK-AUTh certificate when a new key is generated in the card). Suggested to add the word "illegitimate" to the sentence.	Suggested modified sentence: "An issued credential is not modified, duplicated or forged by an ***illegitimate*** party."	Resolved by revising the sentence to "An issued credential is not duplicated or forged, and is not modified by an unauthorized entity."
IDTP-5	IDTP	GL	E	6	410	2.3	List a PIV card as a possible form of identification. This is what is most likely required to issue a second PIV card when a pseudodynm is used (section 2.4.1)	List a PIV credential (card) as a valid form of ID	Accept.
IDTP-6	IDTP	GL	G	8	445	2.3	Allowing to issue PIV cards to foreign nationals means the PIV card is not an identity card for US citizens only. Consequently, there is no guarantee at all that a PIV cardholder is a US citizen and this section may create an open playing field for what PIV meams to other agencies. Without a common identity vetting and criteria for all PIV cardholders, each agency might have to do some verifications of its own, undermining the common interoperable identity card. Using the PIV-I model (issued by a Federal agency) for such foreign nationals would be a much better solution.	Use PIV-I cards (with an ad-hoc OID) issued by Federal agencies to allow foreign nationals to work for the DoD or the Department of State.	Declined. HSPD-12 does not limit the issuance of PIV cards to only US citizens. Instead, it specifies 'common identification'. The use of a different identification for non-US citizens is not aligned with HSPD-12.
IDTP-7	IDTP	GL	G	8	526	2.5.1	The document is referencing 32 times the FASC-N. The FASC-N is used only by PIV cards but not by PIV-I cards. Also when the UUID becomes a requirement in PIV cards the FACS-N may one day be deprecated. It is suggested to introduce early in the document a notion of "credential Identifier" which can be either the FASC-N or the UUID and to use in the rest of the document the term "credential identifier" contained in the CHUID.	Add a definition section around (or before section 2.4) clarifying what the card identifier is (FASC-N) and use the term "card Identifier" thereafter. Indicate the card identifier could be the UUID when the FASC-N value is all nines (9). Indicate the card identifier is used as the binding element between all signed data objects in the PIV card application.	Resolved by NIST-81. Declined - PIV-I is out of scope of this document. Solved by NIST-81.
IDTP-8	IDTP	GL	T	10	549	2.5.2	According to this section, revocation of the digital certificate is optional when the card has been collected. It should be specified this works only when the card is retrieved and is functional. If the card is not functional anymore there is a risk the module of the card has been subsituted by a broken module, allowing the original real module to still be available to an attacker.	Stipulate the revocation of the digital signing certificate is optional only if the card is collected and is authentic and electronically verified as functional before being zeroized.	Resolved by making revocation mandatory in the case of reissuance. (Note: reissuance now exclusively applies to 'lost, stolen, damaged, or compromised cards'.)
IDTP-9	IDTP	GL	T	11	583	2.5.4	This paragraph should mention that the Security Data Object may also have to be updated as a consequence of other updates.	Suggested to add a sentence saying: "The security Data Object in the card shall be updated to reflect any changes made by such modifications".	Resolved by NIST-95.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IDTP-10	IDTP	GL	T	21	862	4.1.2	ISO 7810 does not define anything useful related to card durability. Here is a quote from the standard: 8.7 Durability "Durability of the card is not established in this International Standard. It is based on a mutual agreement between the card purchaser and the supplier." NOTE: ISO/IEC 24789 is now under development and will contain durability tests.	Remove the bullet about ISO/IEC 7810 reference to durability and point to existing durability standards (e.g. ISO/IEC 24789).	Decline to refer to a standard under development. Also, remove reference to [ISO7810] in line 862.
IDTP-11	IDTP	GL	E	33	1091	Figure 4-6	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and indicate in a note that the chip is on the front of the card.	Accept.
IDTP-12	IDTP	GL	T	34	1096	Figure 4-7	The magnetic stripe is on the wrong side of the card if this card has to be ISO compliant. Refer to FIPS201-1 in which the chip is on the top of the card and the magnetic stripe of the left.	Correct the figure by moving either the magnetic stripe to the right or the chip to the top.	Resolved by reverting back to FIPS 201-1, removing references to TSA, DOB, and Gender, adding 'B' to zone numbers. Removed reference to TSA as per resolution on comment number DHS-24.
IDTP-13	IDTP	GL	E	34	1096	Figure 4-7	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and indicate in a note that the chip is on the front of the card.	Accept.
IDTP-14	IDTP	GL	T	35	1100	Figure 4-8	The magnetic stripe is on the wrong side of the card if this card has to be ISO compliant. Refer to FIPS201-1 in which the chip is on the top of the card and the magnetic stripe of the left.	Correct the figure by moving either the magnetic stripe to the right or the chip to the top.	Resolved by reverting back to FIPS 201-1, removing references to TSA, DOB, and Gender, adding 'B' to zone numbers. Removed reference to TSA as per resolution on comment number DHS-24.
IDTP-15	IDTP	GL	E	35	1100	Figure 4-8	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and indicate in a note that the chip is on the front of the card.	Accept.
IDTP-16	IDTP	GL	T	37	1139	4.1.6.1	It is possible to have more than one symmetric key available for PACS using the correct context selection. Defined correctly this requires only one key reference and provides backward compatibility with existing versions of SP800-73	Allow more than one symmetric card authentication key for PACS. **See IDTP detailed comment word document for possible options suggested.**	Resolved by Cert-85.
IDTP-17	IDTP	GL	E	37	1153	4.1.7	"... operations such as reading ...." Technically the card can always read information in its memory, but the privileged operations mentioned here is about a reader trying to access (read) the information.	Suggested to change the sentence as follows: "The PIV Card shall be activated to perform privileged operations such as *allowing the terminal (reader) to access* biometric information ...."	Resolved by DoD-38.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IDTP-18	IDTP	GL	T	38	1186	4.2	It is perfectly correct to say that the signature adds entropy to the unsigned CHUID, but this is not a good reason to assimilate the signed CHUID into a password. The signed CHUID is a public identifier which can be read freely over any interface by any reader without the user's knowledge. This paragraph, as written, would tend to suggest that the signed CHUID could be used for authentication of the user. However, the signed CHUID is only an identifier which provides authenticity of the signer and should be treated as such. It may indeed be good practice to store only a hash value of the CHUID in relying systems, but this section should in no way recommend assimilating to, or using the CHUID as, a password.	Replace the whole paragraph with the following: "The CHUID may be read and used by the relying system and should be treated as an identifer. It provides information about the CHUID issuer and cannot be modified or altered because of its digital signature. But even so, the CHUID (or any part of it) should not be used as an authenticator as it can be duplicated, cloned or replayed even without the legitimate cardholder's knowledge or consent. It can be used as an index pointer in relying systems; but used alone, should never be considered as an authentication factor regarding the user or his/her card."	Resolved by Cert-73.
IDTP-19	IDTP	GL	E	40	1250	4.3	It is a good thing that the CAK Asymmetric is now a requirement, but there should be a timetable, and/or a migration plan indicating how agencies which did not have it before will change their cards and systems that use cards.	Suggested to add a note: "As the previous version of this standard did not make this a mandatory key, relying systems must test for the presence of the CAK certificate and should not reject a card as a false PIV card when this certificate is not present."	Declined. FIPS 201 does not specify any authentication mechanism that involves verifying that every mandatory data object is present.
IDTP-20	IDTP	GL	T	41	1298	4.3	The paragraph about symmetric keys clearly indicates there are commands and containers which are not (and will not be) specified in the FIPS 201 standard. Nevertheless, it should be clearly indicated in the relevant standards which commands, references, container identifiers and so on are available for such additional features. Not mentioning what is reserved for PIV and what is available for additional features is begging for collisions with future updates of the PIV standard that could disrupt previous implementations.	Suggested to modify the last sentence: "This standard does not specify key management protocols or infrastructure requirements, but will provide naming spaces as well as card commands allowing such functions not to interfere with this standard or its future releases."	Declined. As with the currently defined keys, the relevant information will appear in SP 800-73 and SP 800-78. Also, the text in lines 1293-1298 is specific to the symmetric card authentication key (i.e., key reference '9E').
IDTP-21	IDTP	GL	E	42	1321	4.4	*"The facial image is not required to be stored on the card" may be a misleading sentence as the facial image is always stored (printed) on the card.*	Suggested to change the sentence as follows: "The facial image is not required to be stored electronically in the chip of the card"	Declined. The facial image is now required to be stored electronically on-card.
IDTP-22	IDTP	GL	G	51	1597	6.1	The document should mention authenitcations which can be done by external systems using the PIV card as an index to a previously established autentication mechanism. The use of a PIN to System (PACS of LACS) as well as a Biometric on LACS (or PACS) is better than using the CHUID alone. This would establish the base line (ID + Password) form which is where many systems are today and show what can be done in addition to such level of authentication with a PIV card.	Add description for existing ID + Password for LACS (same for PACS with a PIN to PACS) as a basis for low assurance of identity, stressing the fact such authenticators (PIN or Password) should be protected by the relying party and not shared between systems.	This comment is out of scope for FIPS 201-2. FIPS 201-2 only addresses authentication mechanisms using PIV Card. Moreover, these methods are already covered in ICAMSC Federated PACS document.
IDTP-23	IDTP	GL	T	54	1717	6.2.3	It is not clearly indicated in the section that this mechanism does not provide revocation check of the credential, even when the signature is checked.	Suggested to add a bullet indicating: "Does not provide verification of credential revocation against a revocation list published by the issuer."	Resolved by adding a bullet to Section 6.2.3 (now Section 6.2.1) under characteristics: "Does not provide protection against use of a revoked card."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IDTP-24	IDTP	GL	E	55	1727	6.2.3.1	It should be indicated (maybe in a note applying to all mechanisms) in this section that the sequence proposed is not normative and could be modified for optimization purposes. For example, capturing the individual's live fingerprints earlier in the process allows to mask most of the PKI processing time even if he/she is not the legitimate cardholder.	Suggested to add a note attached to bullet 6: "Note: the sequence of operation described in this section may be modified for optimization purposes. For example, capturing the live fingerprint at the beginning of the sequence would shorten the time of the whole verification, as percived by the user, if other processes (such as PKI processing) can be executed in parallel".	Resolved by removing the sequence ordering of authentication mechanisms.
IDTP-25	IDTP	GL	T	55	1738	6.2.3.2	This line states that the PIN entry is verified by the attendant and, as such, seems to imply this provides "more assurance" than for the BIO alone. It is true that the presence of the attendant does help ensure that there is no fake biometric spoofing as stated later. However, it is inappropriate for an attendant to observe the entry of a cardholder's PIN since it is a secret. Also, the entry of a PIN wihtout a cryptographic transfer of trust does not prove that the card is genuine as referenced in SP800-116 Section 7.1.7.	Remove the second sentence on line 1738 (third bullet).	Resolved by removing lines 1735-1749 as per comment DoD-62.
IDTP-26	IDTP	GL	T	56	1751	6.2.3.2	See IDTP comment on Page 55, line 1738, section 6.2.3.2	Change the sentence to read as follows: "This authentication mechanism is similar to the unattended biometrics authentication mechanism; the only difference being an attendant (e.g., security guard) supervises the entry of the live biometric information by the cardholder."	Resolved by modifying the sentence as follows. "This authentication mechanism is the same as the unattended biometrics (BIO) authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder."
IDTP-27	IDTP	GL	T	57	1806	6.2.6	Reading the CHUID is useful for two reasons: Obtaining the diversification number used to calculate the correct derived key for the card and to verify the card expiration date in the CHUID. This must be done if the challenge/response used is very basic (as described in this sequence). When using more elaborate authentication protocols which create a session key, it would be much more efficient (as well as more secure) to exchange card information (such as the date) under a session key protection.	Suggested to add a note indicating that "The protocol shown in this section is for information purposes only. More elaborate protocols could be used when exchanging data using a session key."	Declined. Session key establishment is out of scope for this authentication mechanism.
IDTP-28	IDTP	GL	T	57	1809	6.2.6	There is no mention at all in this section about key diversification in the card and how the terminal calculates the correct key for the presented card.	Suggested to add a bullet after bullet #3 indicating: "The reader calculates the correct key (e.g. diversification) related to the presented card."	Resolved by adding the following text in Section 4.3 (now Section 4.2.2), Symmetric Card Authentication (lines 1293-1298): "If present, the symmetric card authentication key shall be unique for each PIV Card and shall meet the algorithm and key size requirements stated in [SP 800-78]."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IDTP-29	IDTP	GL	T	58	1843	6.3.1 Table 6-2	It is misleading to indicate in this table that VIS or CHUID used alone provide more than "little or no" level of identity assurance/confidence. In SP800-116, only the combination of VIS and CHUID provices some confidence. VIS and CHUID alone should be considered as little or no confidence. Only when used in combination could they provide some confidence.	Add one row in the table for "Little or No confidence" in which VIS, CHUID will be. Change the rwo "Some confidence" to have VIS+CHUID, PKI-CAK.	Resolved by adding a row for LITTLE or NO confidence to include VIS and CHUID. Moreover, we will insert pointer to SP 800-116 for combinations of authentication mechanisms. FIPS 201-2 will say in a footnote: "Combinations of authentication mechanisms are specified in [SP 800-116]."
IDTP-30	IDTP	GL	T	59	1856	6.3.2 Table 6-3	This table assumes the client (local workstation) on which such verifications are made has not been subject to any kind of attack or malware invasion. This should be mentioned as it is VERY important that the PIN or the Biometric data is not captured, cached and replayed in a rogue client.	Add a note under the table: "This table assumes the workstation software and middleware has not been modified or altered by malware".	Resolved by adding the following text to Section 4.4.4, Card Activation Device Requirements. "Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document." Add reference to SP 800-53.
IDTP-31	IDTP	GL	E	60	1857	Appendix A	Should indicate this appendix is normative	Add Normative	Accept by inserting the following text before A.1: This appendix provides compliance requirements for PIV validation, certification, and accreditation, and is normative.
IDTP-32	IDTP	GL	E	62	1934	Appendix B	Should indicate this appendix is informative	Add Informative	Resolved by deleting Appendix B per OPM-6.
IDTP-33	IDTP	GL	E	62	1936	Appendix B	This section describes only the NACI process. It could be useful to also describe the CHRC process.	add a description of the CHRC process to provide a complete example.	Resolved by deleting Appendix B per OPM-6.
IDTP-34	IDTP	GL	E	63	1947	Appendix C	Should indicate this appendix is informative	Add Informative	Resolved by deleting Appendix C.
IDTP-35	IDTP	GL	E	64	1952	Appendix D	Should indicate this appendix is normative	Add Normative	Accept by adding: "This normative appendix provides additional details for the PIV objects identified in Section 4." Note: Two of the appendices have been removed in the revised draft, causing a shift in numbering accordingly.
IDTP-36	IDTP	GL	E	66	1985	Appendix E	Should indicate this appendix is informative	Add Informative	Resolved by adding: "This informative appendix describes the vocabulary and textual representations used in the document. Note: Two of the appendices have been removed in the revised draft, causing a shift in numbering accordingly.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IDTP-37	IDTP	GL	E	69	2116	Appendix E	Definition of Path Validation should indicate in a note that this process alone does not provide a revocation check of individual credentials.	Note: this process alone does not provide a revocation check of individual credentials	Resolved by noting in the descriptions of the PKI-AUTH and PKI-CAK authentication mechanisms that path validation includes revocation checking and by noting in the descriptions of the CHUID and BIO(-A) authentication mechanisms that these mechanisms do not protect against use of a revoked card. Note: The certification path validation algorithms in both X.509 and RFC 5280 include checks that none of the certificates in the certification path are revoked. So, in the case of the PIV Authentication certificate, Card Authentication certificate, digital signature certificate, or key management certificate, path validation alone does provide a revocation check of the individual credential. While path validation for the PIV content signer certificate would not provide a revocation check of an individual PIV Card, a note such as this in the definition of path validation would be misleading since the definition is not specific to the content signer certificate.
IDTP-38	IDTP	GL	T	74	2298	Appendix F	The reference to ISO 7816 without a published date indicates the latest revision of the document is to be used. If this is the case, it should be referenced that SP800-96 used a different reference (ISO/IEC 7816-3:1997) which is not compatible with the latest version of the ISO 7816-3 protocols. Another option is to update SP800-96 accordingly.	See comment on Page 76 Line 2340 in which the change should be done. No action is needed here if the comment on line 2340 is addressed as suggested.	Resolved by IDTP-39.
IDTP-39	IDTP	GL	T	76	2340	Appendix F	SP800-96 calls for a deprecated version of ISO/IEC7816-3 (version 1997) which is not compatible with the latest layer definitions of ISO/IEC 7816. This should be indicated in the list of references or SP800-96 should be updated.	Update SP800-96 to use the current version of ISO/EC 7816-3	Noted. This comment is made against SP 800-96 and as such is out of scope. Our intention is to modify all Special Publications related to PIV as necessary.
IGL-1	IGL	SW	G	6	169	0.9?	"This standard is effective immediately". Some parts of the standard will rely on specifications which will not be published immediately, such as an update to SP 800-73 along with SP 800-85A/B and the associated tools.	"This standard is effective immediately, except where final publication of dependent specifications is required." This seems weak - is specifically naming sections an option?	Resolved by DoD-3.
IGL-2	IGL	SW	E	8	472	2.4	"The PIV Card shall be valid for no more than six years." Needs coordination with GSA regarding durability thresholds: need to confirm if current GSA durability testing criteria are based on 5 year card life; the previous version of the standard did not have this 6 year statement, but indicated 5 years in PIV Card Renewal (FIPS 201-1 Section 5.3.2.1)	3 alternatives: 201-2: "The PIV Card shall be valid for no more than five years." - Or (GSA): Clarify that PIV Card / CPS AP are sufficient to satisfy 6 year card life - Or (GSA): Update the APs (expect vendor pushback)	Resolved by ES-3.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IGL-3	IGL	SW	E	8	476	2.4	"Agencies may reuse them or discard …" Is this policy consistent with page 9 Section 2.5.1 line 519 statement "The original PIV Card must be collected and destroyed"?	"Agencies may reuse or destroy …"	Resolved by Cert-18.
IGL-4	IGL	SW	E	10	548	2.5.2	Awkward wording in first sentence is better stated in second sentence: "Revocation of the Digital Signature Key certificate is only optional if the PIV Card has been collected and zeroized or destroyed. Similarly, the Key Management Key certificate should also be revoked if there is risk that the private key was compromised."	"Revocation of the Digital Signature Key certificate is required unless the PIV Card has been collected and zeroized or destroyed. The certificate corresponding to any on card private key should be revoked if any on card private key is compromised."	Resolved by DOT-15. See also IDTP-8.
IGL-5	IGL	SW	T	11	579	2.5.3	"Only the keys and certificates shall be updated." Shouldn't old certificates be revoked if the corresponding private key is compromised?	"Only the keys and certificates shall be updated, and the certificates corresponding to all compromised keys shall be revoked."	Resolved by ES-30.
IGL-6	IGL	SW	T	11	590	2.5.4	"Communication between the PV Card issuer and the PIV Card shall occur only over mutually authenticated secure sessions between tested and validated cryptographic modules (one being the PIV Card)." This statement makes the status quo a requirement; but how will this requirement be enforced? this type of function has so far been out of scope of SP 800-73-3. It is in scope of FIPS 140-2, but there is typically no method to enforce the presence of a feature like this. This comment also applies to the bullet at line 592.	Keep this statement in FIPS 201-2. Add an Appendix with required PIV Card features or Security Policy content. Consider a Security Policy "profile", similar to the idea of a Common Criteria Protection Profile for expected features (like this) and dependent algorithms (like SP 800-56A ECC CDH Section 5.7.1.2 if 9D is supported).	Resolved by ES-5.
IGL-7	IGL	SW	T	11	596	2.5.4	"If the PIV Card post issuance update begins but fails for any reason, the PIV Card issuer shall immediately terminate the PIV Card as described in Section 2.5.6, and a diligent attempt shall be made to collect and destroy the PIV Card." This seems drastic - is recovery in this scenario untenable? Also, in what circumstances would the issuer not have possession of the card for an update?	"PIV Card Issuers shall implement a post issuance update failure policy. If the PIV Card post issuance update begins but fails for any reason, the PIV Card issuer shall carry out that policy, potentially including immediate termination as described in Section 2.5.6 and destruction of the PIV Card."	Resolved by DoD-27.
IGL-8	IGL	SW	T	12	603	2.5.5	See comment re Section 6.2.5. The statement in this section should apply to either PIN or any retry counter for a biometric used as a PIN alternative.	Add a sentence following the first sentence in this section, near the end of line 606: "Similarly, the need to reset authentication data retry counters also applies to any biometric authentication mechanism used as a PIN alternative." Modify the next sentence to read: "PIN **or biometric authentication data retry count** resets may be performed by the card issuer."	Declined – The second paragraph in section 2.5.5 (now Section 2.9.4) addresses the requirement for resetting biometric data. These requirements are different from PIN reset and should not be combined.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IGL-9	IGL	SW	E	12	619	2.5.5	"… requiring the termination of PIV Cards that have been locked." In this context, does "locked" mean PUK retries are exhausted? Suggest clarification of this point.	"… requiring the termination of PIV Cards blocked by exhausted PUK retry count." Alternatively, define a term for this in the Glossary; "lock" seems overloaded with several possible meanings including: the low level card transport lock; VERIFY not yot performed; blocked on PIN retry count = 0t; blocked on PUK retry count = 0).	Resolved by removing use of word 'locked'.
IGL-10	IGL	SW	T	21	882	4.1.3	"… temperature and humidity-induced dye migration, …" This section of 201 lumps together issues that are card durability and the effects of printing on the card. This particular item is one example of a test that was sorted into the CPS category. The issue of card body qualification and printer effect qualification should be straightened out in this version of FIPS 201-2.	Suggest a small group effort to restate this section.	Resolved by ES-8.
IGL-11	IGL	SW	T	21	884	4.1.3	"Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water mixture. The reagents called out in Section 5.4.1.1 of [ISO10373] shall be modified to include a two percent soap solution." This statement is obscure and long been the source of confusion, and should be reworded. The hand cleaning requirement and separate statement about exposure to soapy water are essentially redundant.	"Card durability testing shall include contaminant exposure in accordance with [ISO10373] Section 5.4.1.1. In addition to these contaminants, cards shall not malfunction or delaminate after hand cleaning with a two percent soap and water mixture."	Resolved by ES-9.
IGL-12	IGL	SW	T	21	915	4.1.3	"The PIV Card may be subjected to additional testing." This sentence too subjective to have any meaning. Remove it.	Delete this line.	Resolved by AI-4 and ES-10.
IGL-13	IGL	SW	T	37	1141	4.1.6.1	"One or two iris images" is listed as optional, but in several places in FIPS 201-2 and SP 800-76-2, iris image is listed as a mandatory feature to be supported if fingerprint cannot be used. See also line 1132 that lists two iris images. The iris container must be mandatory to support iris as a mandatory backup to fingerprint.	Remove this item from the Optional section; add it to the mandatory section underneath line 1132.	Declined. Since release of the FIPS 201-2 draft, the decision is that iris is now optional, so this change is not necessary.
IGL-14	IGL	SW	T	37	1142	4.1.6.1	"On-card biometric comparison data" It is not clear in 201 that there are two different containers for fingerprint; one for on-card, one for off-card. SP 800-76-2 does refer to some template differences; and as a container, GET DATA access requires PIN verify while on-card biometric comparison does not. But is this separation necessary? It may take up additional card memory at the expense of other features, such as retired keys.	Need to clarify 800-76 rationale for separate containers.	See ES-12.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IGL-15	IGL	SW	T	37	1144	4.1.6.1	"PIV logical credentials fall into the following three categories:" See associated paper on authentication strength, and comment on 6.2.5. It would help to expand on the purposes of authentication in this section.		Declined. The three uses outlined in the paper are equivalent to cardholder-to-card authentication, which is already covered in FIPS 201-2.
IGL-16	IGL	SW	T	37	1150	4.1.6.1	"The PIN falls into the first category, the card management key into the second category, and the CHUID, biometric credential, symmetric keys, and asymmetric keys into the third." See comment on 6.2.5. With introduction of on-card biometric comparison, if it is a PIN substitute, biometric is also in the first category.	"The PIN **and on-card biometric comparison data fall** into the first category, the card management key into the second category, and the CHUID, biometric credential, symmetric keys, and asymmetric keys into the third."	Add sentence below 1151: The fingerprint templates for on-card comparison fall into the first and third categories.
IGL-17	IGL	SW	E	37	1152	4.1.7	The term "Activation" seems awkward and misleading, as suggested by footnote 8. The topics seems to be about controlled access to card functionality.	Consider wording similar to: "4.1.7 Controlled Access to PIV Card Functions Access to privilieged PIV Card functions shall be granted after authentication …".	Declined. The term "activation" has been used in FIPS 201-1, many other related documents (Roadmap), and is generally accepted.
IGL-18	IGL	SW	T	37	1168	4.1.7.1	"The required PIN length shall be a minimum of six digits." See discussion of authentication strength in the attached paper.	Workable if retry count limited to 10 to satisfy FIPS 140-2 AS03.26 when used with DSK or KMK. However, consider alternatives such as expansion of Discovery Object function to improve the overall security and allow greater flexibility for appropriate selection of PIN policy.	A discoverable PIN policy is counter to interagency interoperability, would not be backward compatible, and would add complexity and cost.
IGL-19	IGL	SW	E	38	1185	4.2	Please provide a reference for the source of this statement: "… (since the digital signature provides entropy equivalent to a password)."	Add a footnote with a reference.	Resolved by Cert-73.
IGL-20	IGL	SW	T	39	1231	4.3	"… keys used to establish a secure messaging …" FIPS 201-2 makes only vague references to secure messaging, but it appears to require secure messaging in relation to on-card biometric data enrollment. This issue merits its own section. Realistically, all cards support secure messaging mechanisms. It would be good to make this available as an option; delivery of PIN in the clear is the factor that limits PIV cards to FIPS 140-2 Level 2. Perhaps line 1500 is calling for this behavior?	Please add a section on secure messaging. Suggest a small group with representation or review by vendors, labs, CMVP, NPIVP.	Resolved by ES-14.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IGL-21	IGL	SW	T	40	1236	4.3	"Where digital signature keys are supported, the PIV Card is not required to implement a secure hash algorithm. Message hashing may be performed off card." Currently, it ***MUST*** be true that hashing is off card, or the function will not be interoperable; a card that performs on-card hashing will fail NPIVP testing as it will get the wrong result. But it would be good to add support for on-card hashing, perhaps in the form of an additional tag. Currently, off-card hashing means the digital signature operation does not support the non-repudiation property. Until PIV, an operation without integral hash was considered by CMVP not to be a true digital signature. Cards have memory limitations, but for some purposes - like signing records by agents - non-repudiation is an important feature.	Add a tag for on-card hash in SP 800-73 and explain clarify this section accordingly.	Declined. As long as off-card hashing is possible, a relying party would not be able to distinguish between a digital signature created using on-card hashing from a digital signature created using off-card hashing.
IGL-22	IGL	SW	T	40	1256	4.3	"The key management key is an asymmetric private key supporting key establishment and transport, and it is optional. This can also be used as an encryption key." Please clarify.	"The key management key is an optional asymmetric private key supporting key decryption (when used with RSA) and shared secret generation (when used with an ECC key to implement the ECC CDH primitive). The key management key is not used to establish keys on the PIV Card."	Resolved by ES-29.
IGL-23	IGL	SW	T	41	1302	4.3	"Private key operations may not be performed without explicit user action." This is the one place where PIN ALWAYS is required; it seems much more important to be clear about the meaning of explicit user action here than to state in the PAK and KMK usage explanations what is not required.	"Private key operations may not be performed without explicit user action - the PIN shall be verified immediately preceding any use of this key."	Resolved by ES-16.
IGL-24	IGL	SW	T	42	1330	4.4	The paragraph starting at line 1330 gives further indication of separate containers for on-card and off-card biometric. There are indicators of differences in SP 800-76-2, but it is not clear how this data is actually a different than the on-card template.	Please clarify how on-card and off-card biometric data differ. Is the issue a container with different access control? Is the data substantively different?	Accepted per ES-17.
IGL-25	IGL	SW	T	47	1500	4.5.4	"If the PIN input device is not integrated with the reader, the PIN shall be transmitted securely and directly to the PIV Card for card activation." Appears to be an option for secure messaging use when PINs are transmitted. Good!	Please add a section on secure messaging. Suggest a small group with representation or review by vendors, labs, CMVP, NPIVP.	Resolved by ES-19.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IGL-26	IGL	SW	T	51	1621	6.1.1	Relationship to OMB's E-Authentication Guidance Should there be a relationship to SP 800-63? It seems more in depth and has similar provisions.	Clarify relationship to SP 800-63 if possible.	Declined. This reference is redundant since FIPS 201 authentication mechanisms follow SP 800-63 general guidelines.
IGL-27	IGL	SW	T	54	1701	6.2.3	Authentication Using PIV Biometric These use cases are the driving factor in a numeric only limitation on PIN, which has the side effect of lowering security for other cardholder authentication.	See 6.2.5 comment and attached paper on authentication strength.	OCC, when used for card activation, has to satisfy the requirements of FIPS 140.
IGL-28	IGL	SW	T	56	1760	6.2.4.1	If on-card biometric is a PIN alternative, it should be listed here.	Add on-card biometric authentication after line 1761.	Resolved by the following changes: - Combine steps 2 and 3. - Add a sentence – If implemented, other card activation mechanisms, as specified in [SP 800-73], may be used to activate the card. - Change the characteristics to - Strong resistance to use of unaltered card by non-owner since card activation is required.
IGL-29	IGL	SW	T	57	1792	6.2.5	"A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC) authentication and the card with an indication of the success of the on-card biometric comparison. The response includes information that allows the reader to authenticate the card. The cardholder PIN is not required for this operation." These sentence do not seem clear that on-card biometric comparison is an alternative to PIN regarding card state. However, SP 800-76-2 is, stating on line 325:"Indeed, FIPS 201-2 extends on-card comparison as an alternative to PIN entry in altering the state of the PIV card." This is an important point to be clear on.	"A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC) authentication and the card with an indication of the success of the on-card biometric comparison. **Successful on-card comparison is an alternative to PIN entry in altering the state of the PIV card.** The response includes information that allows the reader to authenticate the card. The cardholder PIN is not required for this operation."	Declined. While card activation may be a side effect of OCC authentication mechanism, this section is specifying an authentication mechanism rather than card activation. See Section 4.1.7.1 (now Section 4.3.1) for alternate ways of activating the card.
IGL-30	IGL	SW	G	?	?	?	Perimeter control devices are in existence - e..g handhelds. They are not defined as a GSA category because they are not mentioned in FIPS 201-2 documentation.	Add a section mentioning perimeter control devices and mobile devices that may be used for both physical access control scenarios and logical access control (mobile access to networks).	Resolved by ES-24.
IGL-31	IGL	SW	T	61	1914	A.4	Current wording clarifies the more blanket statement made in FIPS 201-1. But what about other types of devices that perform crypto? They too should have a FIPS 140-2 cert per FISMA - at what level?	Convene a small group to address this section. What Level(s) makes sense for each category? By default, GSA APs call for Level 1 - this may make sense in some cases. This is an issue worthy of more examination.	Resolved by ES-25.
IGL-32	IGL	SW	E	75	2328	F	SP 800-73-3 is cited, it is not in line with this standard. This also pertains to the issue of immediate enforcement of this standard on adoption.	Include a note about SP 800-73-4 and SP 800-85A-3 development, and the short term solution of some card comands in SP 800-76-2.	Resolved by ES-26.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
IGL-33	IGL	SW	E	75	2330	F	SP 800-76-2 is in draft, and will be in force when this is in force.	Cite SP 800-76-2.	Resloved by ES-27.
KAA-1	Kelly-Anderson & Associates	John Mercer	G		853	4.1.2	The current draft specifies a minimum of one security feature (Line 853) and further specifies that two of the security feature options be a commercially available technology (hologram and holographic images) that are often subject to counterfeiting or simulation because holographic technology is readily accessible from organizations that are not involved in the production of security documents	Our suggestion is to expand and qualify this requirement by requiring that a minimum of two such devices/techniques be used on the face of the card and that they be of different visual technologies, such that ability to emulate one would not compromise the second. Furthermore, we recommend that the term hologram be re-specified as an Optically Variable Device incorporating diffractive structures and technology that are only available from high security manufacturers. We further suggest that the same distance criteria applied to the detection of the basic card stock color (50cm-200cm) be applied to the detection of the appropriate optical activity of the optically variable device. This is in large part to address facility entry/automobile access, where the card is not subject to electronic systems verification as it is in logical access situations. Use of this distance criteria – in such a flash pass environment – would place an emphasis on the visually unique characteristics of such a feature, and also place a premium on the optical return or visual play-back from the optically variable device. We would be pleased to meet with NIST on a confidential basis to further discuss the technical attributes of optically variable technology and how it is used by numerous government agencies to protect their most sensitive identification products.	Declined. Since the VIS authentication has been downgraded to "Little or No Confidence", the increased cost of additional printed security features would not be justified.
LLNL-1	LLNL - S&P	Mike Mercer	T			4.2	This section says the CHUID should not be stored. Since the FASC-N portion of the CHUID is recommended for use as the unique identifier for PACS, this section cannot preclued storing the FASC-N. This should be clarified.		Resolved by removing the third paragraph of Section 4.2 (now Section 4.2.1), lines 1184-1187.
LLNL-2	LLNL - S&P	Mike Mercer	T	54		6.2.2	Most sections specifically call out the FASC-N as the unique identifier. This seciton does not. If the intention is for future use of the GUID in addition to or instead of the FASC-N, this should be clarified.		Resolved by NIST-81.
LLNL-3	LLNL - S&P	Mike Mercer	T	54		6.2.3	DOE has used hand geometry for biometric authentication for many years. FIPS 201-2 should recognize hand geometry authentication as an acceptable alternative to fingerprint or iris authentication.		Declined. Current commercial hand geometry implementations are proprietary, non-interoperable, and include a database of enrolled templates in the device. It is not clear what data would be stored on a PIV Card currently. See also IBIA-4.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LLNL-4	LLNL - S&P	Mike Mercer	T	56		6.2.4	For certificate authenticaiton, there is a requirement to check for certificate revocation. This is difficult since many PACS systems are on closed networks, and do not have direct access to online CRLs. Revocation needs only to be as current as the most recent CRLs. We recommend FIPS 201-2 be modified to allow revocation checking using CRLs up to 24 hours old, to facilitate a convenient daily cycle for retrieval of CRLs and processing revocation cheching on badges enrolled into PACS.		Resolved by deleting the word 'online' from "Requires the use of online certificate status checking infrastructure." See also FAQ 53 in OMB Memorandum M-11-33, which states: "Revocation checking may be accomplished by 'caching' revocation information from the credential issuer provided the cache is refreshed at least once every 18 hours."
LLNL-5	LLNL - S&P	Mike Mercer	T	58		Table 6.2	We believe the requirement to obtain VERY HIGH Confidence is inadequate. PKI-AUTH is not equivalent to BIO or BIO-A in that it does not bind the badge holder to the badge except by the easily obtained PIN. We recommend this table entry be modified to require BIO or BIO-A and PKI-AUTH.		Declined. We would like to maintain consistency with SP 800-63,which requires two factors of authentication for VERY HIGH assurance level. We note that Table 6-2 defines the minimum requirement for each assurance level. FIPS 201-2 Section 6.3, introductory paragraph already says "Two or more complementing authentication mechanisms may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder. For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in cardholder identity."
LLNL-6	LLNL S&P	Mike Mercer	T	57		6.2.5	We do not believe on-card biometric authentication is wise. If PIV cards are hacked such that bogus cards can be made, external biometric authentication is the only protection against an attacker. We recommend the on-card biometric authenticaiton be eliminated.		Declined. Both off and on-card biometric authentication is available with the PIV card. When OCC Authentication mechanism is used, the card is authenticated, which precludes the use of a bogus card.
LLNL-7	LLNL S&P	Mike Mercer	G	58		6.3.1	Physical Access Control Systems (PACS) for high security applications are most often configured in concentric layers: increasing confidence being required as a person progresses towards higher consequence targets. Once a user and credential have sucessfully passed an authentication check at an outer level, FIPS 201 should not require that authentication check then be repeated at the next higher confidence level, it should be allowable to take credit for the successful outer layer authentication. Validation of additional factors might be required at inner boundaries, as required but not repeating outer layer checks within a defined window of time.		Nothing in FIPS 201 precludes the use of authentication mechanisms as described in this comment. In fact, this approach is described in SP 800-116.
LLNL-8	LLNL S&P	Mike Mercer	G	58		6.3.1	No consideration has been given as to the slow performance of the PIV-II credential in executing the more intensive authentications and the impact that will have on a typical PACS. Some balance, based on a risk-benefit analysis, should be allowed between the need for higher credential assurance and lower throughput. The changes between this revision and the prior, making all PKI validation mandatory will have tremendous performance consequences.		As described in SP 800-116, the PKI validation does not necessarily need to be performed on-demand. See OMB Memorandum M-10-15.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LLNL-9	LLNL S&P	Mike Mercer		54		6.2.2	Approved contactless readers currently on the market for PIV are not capable of returning the CHUID signature Systems currently being designed and tested are being designed to accommodate this at a later date.		Noted.
LS3-1	LS3 Technologies	Stuart Moisan				General	As a general concern, what assurance do PIV system developers have that requirements expressed in NIST-authored publications will be in accordance with accreditation requirements?		Noted. NIST published SP 800-79 for PCI accreditation guidelines. It is out of NIST's scope how the SP 800-79 controls are implemented by agency.
LS3-2	LS3 Technologies	Stuart Moisan		358, 454, 2137			Assuming that the Sponsor is the originator of the authorization for issuance of the credential, please clarify whether or not the Sponsor role as request originator is distinct from Registrar and Issuer roles, and thus may serve as one of the roles in the 2-role minimum mandated by the Separation of Roles/Duties requirement.		Please see clarification provided in IDmanagement.gov website -- FAQ # 7 at http://www.idmanagement.gov/documents/hspd12_faqs_implementation.pdf.
LS3-3	LS3 Technologies	Stuart Moisan		366			Please clarify in line 366, providing criteria the satisfaction of which gives sufficient assurance that 1) the person undergoing identity-proofing is 2) the person whose biometric(s) are employed in the background check is 3) the person to whom the credential is issued. The first and third cases will often occur in separate instances as they concern Registrar and Issuer functions respectively. The second may occur in a separate instance and indeed may occur prior to the PIV Registrar capture of the biometric used on the PIV card.	Suggestion is that it should be possible for a separate organizational unit, such as a Security Background Investigation Office or an Employee (Contractor, Affiliate, or Volunteer) on-boarding office, to either submit a request for or perform the NCHC check (as well as other generic checks required for employment at the VA in addition to specific checks required by the security classification of the Applicant's employment position) prior to the Sponsor-submitted authorization for a PIV card. Suggestion is that as long as the Registrar can match the biometric used in the background check against a live sample presented to the Registrar during the Applicant's in-person appearance, and/or the identity source documentation presented by the Applicant matches that used in the background check , there is no loss in level of authentication assurance between the Applicant for whom the background check was performed and the Applicant undergoing PIV credential registration. This would have the additional benefit of allowing a Security Background Investigation Office to employ whatever biometric technology is appropriate for its function independently of the biometric technology most appropriate for PIV card functionality. Please see below.	Declined. The standard does not define specific implementation process but the requirements for overall credential issuance.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LS3-4	LS3 Technologies	Stuart Moisan			369		Please clarify the line 369 vis-à-vis the Separation of Roles/Duties requirement. The same lack of clarity is in [SP 800-79]. It appears that the intent of this publication and others is that no single administrator shall have the capability to perform all the tasks required in the end-to-end process comprising an instance of PIV card credentialing. It appears that a valid interpretation of 369 above is that enforcement, presumably by system security controls, shall be such that the issuance of a PIV credential is impossible without a proper request. This makes the Sponsor-submitted request for a PIV credential the start of the process.	Suggestion is therefore that the Sponsor role count as one of the roles under which an administrator may act in satisfaction of the Separation of Roles/Duties requirement. Assuming, for example, that the roles of Sponsor, Registrar, and Issuer are required for each PIV card credentialing instance, two administrators may divide their work between these roles in a way that best meets their resource needs in performance of a given PIV card credentialing instance. For organizations whose PIV facilities are limited in staff, this will allow them to meet the Separation of Roles/Duties requirement with considerable flexibility.	Noted. The intent is a two-way separation of role without specifying a particular implementation. Please also see idmanagement.gov website -- FAQ # 7 at http://www.idmanagement.gov/documents/hspd12_faqs_implementation.pdf.
LS3-5	LS3 Technologies	Stuart Moisan			372		Please clarify the above as regards corrupt official and credential issuance. Ambiguity allows this requirement to be interpreted in a way that does not preclude a non-corrupt official from issuing a credential with an incorrect identity…	Suggestion is to rewrite the above requirement. Suggestion is to define credential issuance in this context as the end-to-end process of PIV card credentialing, beginning with the request authorization and ending with the Applicant in full, officially documented possession of a PIV credential. It could be useful to distinguish card issuance from something like card credentialing/commissioning. Card issuance would then be restricted to the last leg of the end-to-end process. Card commissioning would apply to the entire process. Suggestion is to separate the above requirement into three requirements to remove ambiguity: 1) It shall not be possible for an instance of PIV card credentialing/commissioning to be performed by fewer than two officials. 2)No PIV card shall be commissioned without a high level of assurance that the card-resident identity is the true identity of the subject. 3) No PIV card shall be commissioned without the subject having the proper entitlement to it. Suggestion is to then link items 2) and 3) to sections explicating "high level of assurance" and "proper entitlement", respectively.	The bulleted list in Section 2.1 specifies the control objectives, and the requirements to meet them are provided in the following sections. See also WM-3.
LS3-6	LS3 Technologies	Stuart Moisan			386, 457		Please provide criteria the satisfaction of which gives an appropriate level of assurance that the PIV card Applicant is in fact the person to whom the successfully adjudicated NACI belongs.		Declined. FAQ 15 in http://www.idmanagement.gov/documents/hspd12_faqs_policy.pdf indicates how departments and agencies may verify that whether a NACI (or equivalent) has already been completed on an existing employee or contractor.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LS3-7	LS3 Technologies	Stuart Moisan			390		Please clarify the term "issuance". Throughout this publication it may mean either the entire end-to-end process, from request to newly minted card to documented and acknowledged possession of a working-order PIV credential, or the last leg of an end-to-end process generally defined by Request, Registration, and Issuance. Does 390 mean that the Applicant must appear at least once before the last leg or at least once for the entire process? If once for the entire process, assuming the Applicant must appear in-person for identity-proofing and biometric(s) capture (which presumably is the Registrar stage), then no appearance would be required in the Issuer stage. The administrator acting in the role of Issuer, however, is the PIV official overseeing the full breadth of the Issuer stage – not just card printing and personalization. If the Applicant is not required to make an in-person appearance before the Issuer, the question is how the Issuer will be able to see his responsibilities through to their end, which requires an official act of acceptance of the credential by the Applicant (per non-repudiation), and an official act of recognition of that acceptance by the Issuer. In order to ensure completion of this phase in a controlled and timely manner, it would appear necessary for the Applicant to make an in-person appearance before the Issuer (or an Issuer delegate in cases of remote delivery). For the sake of clarity, suggestion is to distinguish a PIV facility appearance from Registrar and Issuer Office appearances. The Applicant will then be required to make an in-person appearance at both Registrar and Issuer offices (broadly understood to allow for remote delivery), but may be able to achieve both in a one-time visit to a PIV facility.		Declined. The 'at least once' requirements is meant to allow agency specific implementation flexibility in issuing credentials. Being more specific limits implementations to a particular issuance process.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LS3-8	LS3 Technologies	Stuart Moisan			438, 463		Please clarify both of the above vis-à-vis identity-proofing, Separation of Roles/Duties, and "issuance process". In 438, it appears that "issuance process" is the last stage of the PCI end-to-end PIV card credentialing process. Yet in the same sentence the phrase "capability to issue" appears to apply to the entire end-to-end process. In 463, it is difficult to guess whether "issuance process" and "issuer" relate to the PCI itself or the last stage of the PCI process (or a single administrator in the role of Issuer performing the duties of that stage). The missing component above is the authorization request, as submitted by "the appropriate authority" (463). Authorization, as communicated in an authorization request, requires identity proofing (as a precondition) no less than registration. Thus, again, the suggestion is that the Sponsor (as the role authorized to submit requests) be admitted as a role in the Separation of Roles/Duties requirement. As background for this and other comments, biometric capture in itself is not identity proofing, as most persons will not have a link between their biometric data as captured and biographic data (including relational data around family, friend, acquaintance, organization, or society) existing in official databases outside the database involved in the capture instance.		Decline to make changes in the document. Please see Section 3.2, PIV Card Lifecyle, for the clarification on PIV card request, identity proofing and registration, and PIV card issuance.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LS3-9	LS3 Technologies	Stuart Moisan			461		The above phrase " chain-of-trust" appears a number of times in this document. Please provide clarification. Precisely at what point is it created? What are the conditions that break it? What are its requirements, and how do they relate to assurance levels around identity-proofing, biometric capture, transmission, and storage, and the PIV credential? The introduction of the concept in this publication is welcomed, but there is considerable work to be done for it to become usable. The publication either states or implies in a number of places that a biometric match alone is sufficient to establish a connection to an existing chain-of-trust. Yet a chain-of-trust is the ground on which everything else depends, including access control enforcement point processing. An organization may require multi-factor authentication for every access challenge. The ability to connect to an existing chain-of-trust in such cases by means of a single factor would clearly undermine that trust.	Suggestion is that the entire end-to-end process of identification, from on-the-street unknown to new-hire in possession of a PIV card, should be revisited in light of this chain-of-trust concept. What exactly does an organization gain in terms of overall assurance of identity after a fingerprint lookup in a set of criminal history databases returns a "no match" condition? The identity is no more established than before the lookup. Presumably this would be the case for the majority of persons undergoing PIV card credentialing prerequisites processing. On the other hand, if there is a match and an associated name and other biographic information, what is known about the assurance level of that information? If the information does not agree with what is presented during identity-proofing, there will need to be an investigation into either a data entry error or fingerprint or identity fraud. This could occur at either end, the identity-proofing sampling end or the reference source end. This publication seems to treat a biometric as the strongest link in the chain. Yet it is easy to imagine cases in which it is the weakest link. It cannot be assumed that the technology to record a biometric will be able to outrun the technology to tamper with or counterfeit it. Presumed live samples, especially those not witnessed by a proper authority, are just data. Depending on the organization's assurance level needs, connection to an existing chain-of-trust could well require presentation of a secret (or responses to well-designed, randomized historical KBA challenges), presentation of the set of identity source documents (or authoritative substitutes) by which the chain was originally begun, and presentation of one or more biometrics. It could also require one or more authoritative testimonials to corroborate the connection, and investigation into the nexus of relationships at the levels of family, friend, acquaintance, organization, and society. Each chain-of-trust will have a level of assurance that is pegged to the purpose it serves. A chain-of-trust cannot be evaluated outside this context of use. Beyond that, however, the chain-of-trust concept, including its framing of trust relationships, is due a careful re-examination. It might prove useful to introduce the concept of a fabric of identity the strength of which is based on the arrangement and preponderance of a multitude of relatively weak fibers.	Resolved by revised text, which provides suggestions for data to be stored in the chain-of-trust and which more clearly specifies requirements for reconnecting to chain-of-trust.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LS3-10	LS3 Technologies	Stuart Moisan			465		Please clarify. Is this issuer a single administrator in the role of Issuer, the issuance component of the PIV system, the Issuer Office within a PCI Facility, the PCI itself, or some other entity? If the issuer in this case is an administrator, then presumably the Applicant must make an in-person appearance before the issuer (or issuer delegate) so the issuer can officiate over the match performance.		Decline to make changes in the document. Note that the response to the query depends on the specific implementation. The requirements in this standard can be met in many different ways.
LS3-11	LS3 Technologies	Stuart Moisan			473		Please clarify the term "delivered". Can a status of "card delivered" be entered into the official record when there is no official oversight of receipt? Can a card be considered delivered even though the Applicant has not performed the commencement reset of the card-resident PIN, or the Applicant has not signed off on the terms and conditions of use, or has not signed for receipt of the card? What is the standing of assurance of delivery completion and non-repudiation as regards card delivery?		Resolved by removing all uses of the term “delivered” from FIPS 201-2. See Cert-18 and NIST-42.
LS3-12	LS3 Technologies	Stuart Moisan			509		Please clarify the term "issuer". Is this the organization's PCI, the PCIF, or an administrator in the role of Issuer? Authorization for renewal should be with the Sponsor, as the official who signs and submits the authorization for renewal. This function requires that the Sponsoring official verify the standing and personal records of the Employee (Applicant). So while the Issuer may do these things, the Sponsor must do them.	Suggestion is that the strength of the "chain-of-trust", as established within the organization by means of security controls (including authoritative oversight, capture of identity and employment support documentation, digital signing, data and record referential integrity, and secure storage and transport ensuring continuity from identity intake processing to PIV card credentialing request origin through request receipt), should be such that there is no need for the Issuer to do these things.	Declined. The document specifies the requirement and does not say how the requirements are implemented.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LS3-13	LS3 Technologies	Stuart Moisan			536			Suggestion is that the above be rewritten to remove requirement that card-related biometric data be stored off-card, presumably in the PIV Card Credentialing system. Assuming that biometric data relating to the criminal background check is not available, and a facial image *biometric* is not available, suggestion is that connection to a chain-of-trust should still be possible by Applicant presentation of the original identity source documents. This is not the same context as that of first-time presentation. It can be required that the documents be the same as the original, as referenced by scanned images as well as computer-searchable text stored in the IDM, on-boarding, or HR system. Presumably the primary document contains a photo and descriptions of other physical traits such as age, height, and weight. When considered in conjunction with the use of secret or KBA challenges, this begins, ceteris paribus, to look like a case of three-factor authentication.	Decline, see the rational of WM-9.
LS3-14	LS3 Technologies	Stuart Moisan			585		Please consider this in connection with 390 and 465 above. If re-issuance is just issuance done over again in the context of credential continuity maintenance, and issuance requires an in-person appearance, then it may be that re-issuance should too. Post issuance *update*, however, is categorically different. The cardholder has possession of a card that is in working order. The identity of the cardholder and the card is known. The changes made to the card are known. This is not a case in which another card replaces an unusable (damaged) card still in the possession of its cardholder or a lost/stolen card not in the possession of its cardholder. It is a case of card update. It is one and the same card undergoing a controlled and observable change. The point here is that remote post-issuance activities are perfectly supportable. They should not be categorized with re-issuance activities, which may or may not be remotely supportable.		Noted. Post-issuance updates are addressed in Section 2.5.4 (now Section 2.9.3) and are not categorized with reissuance activities. Remote post-issuance updates are explicitly allowed.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LS3-15	LS3 Technologies	Stuart Moisan			607		Please clarify "issuer". Is this a system? If it is an administrator in the Issuer role, the verbiage that follows it about more stringent procedures including in-person appearance would not be needed. If it is a system, and match on-card is not available, then the system must be able to access the biometric on the card without a valid PIN entry (which, though technically possible, has not been discussed at all). The way this requirement reads, it appears that the issuer is an administrator, in which case the cardholder is already making an in-person appearance.		Resolved by revised text.
LS3-16	LS3 Technologies	Stuart Moisan			615		Here there is a possibility of using identity source documentation for connection to an existing chain-of-trust. The use of identity source documentation for chain-of-trust connection should be consistent throughout the publication. If there is a substantive difference between this case and others, please clarify how that difference justifies the use of such documentation here but not elsewhere.		Resolved by DoD-54, DOT-11, DOT-18, and GSA-17.
LS3-17	LS3 Technologies	Stuart Moisan			965		Please clarify the format above. The year and day is numeric, while the month is alpha. I don't recall reading about a month *abbreviation* anywhere in the publication.		Resolved by adding the following text to the sentence in line 965: "whereby the MMM characters represent the three-letter month abbreviation as follows: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, and DEC."
LS3-18	LS3 Technologies	Stuart Moisan			1155		Please clarify. This seems to be putting the cart before the horse.		Declined. Commenter does not explain why requiring cardholder or card management system authentication before activating the card for privileged operations "seems to be putting the cart before the horse."
LS3-19	LS3 Technologies	Stuart Moisan			1275		Please provide more information if possible.		Declined. The referenced text states that the expiration date of the PIV Authentication certificate must be no later than the expiration date of the PIV Card. The commenter does not specify what additional information is needed or the reason for believing that additional information is needed.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
LS3-20	LS3 Technologies	Stuart Moisan			1317		Please clarify biometric requirements. On the one handI, the first entry mentions a full set of fingerprints. The last entry allows for no fingerprints. There is also the question of the storage of biometrics. Are there any requirements for off-card storage of biometric data? Please specify which data if so. Finally, allowance should be made for law enforcement to use one biometric minutiae format, biometric technology, or biometric and the PIV card another. What may be appropriate for law enforcement checks may not be the most appropriate for PIV cards. Furthermore, even if technical specs were identical, it may be desirable to allow the biometric capture for law enforcement to be separate from the biometric capture for PIV card processing. An organization should have the option of performing a law enforcement check prior to submitting the request for a PIV card. If the biometric is of the same type between the two, and either the minutiae match directly or after appropriate conversion, that should be enough to establish sameness.	General suggestion is to require that the biometric and identity source documentation held by the subject match the reference biometric and support documentation held by the challenging system. This also allows for greater flexibility in choice of PIV card biometrics. If there is a match between a card Applicant and a law enforcement record as regards fingerprint, and there is a match between the same card Applicant and a PIV card record as regards, say, iris- and voice-print, it would not be unreasonable, ceteris paribus, to conclude that the law enforcement record and the PIV card record belong to the same person. Please see above. FIPS-201-2 comes close to allowing for this in footnote 11 in section **4.4.1 Biometric Data Collection and chain-of-trust.**	Resolved by the following: Note that format for fingerprint for PIV Card and law enforcement are different and footnote 11 (now footnote 3) already suggests that they may be collected at different times. So, FIPS 201 already allows differences. Biometrics collected for law enforcement and stored on PIV Card are matched to ensure it belongs to the same person. So, FIPS 201 already accommodates the matching requirements. Add clarification to the first bullet to explain that if a full set of prints cannot be collected, then as many prints as available shall be collected. Break up Section 4.4 such that biometric data collection and biometric data stored on the card is specified separately.
LS3-21	LS3 Technologies	Stuart Moisan				General	Frankly, this draft publication seems to contain more than one version. It would be a great help if obsolete material were removed.		Declined. No instances of obsolete material are provided.
LS3-22	LS3 Technologies	Stuart Moisan	G			General	Per card topography: Yes, please split prefixes and suffixes (and generational title) from first, middle (full or initial), and last name. According to what I'm hearing, there could be a name field like: Smith, Jim Jr. Need to know that "Jr." is a generational title, and not, say, a middle name abbreviations.		Declined. "Jr" is an example and there are many more possibilities. The set of interpretation is too large to be addressed in FIPS 201.
NASCIO-0	NASCIO	Chad Grant / Doug Robinson					See PDF Attachment for all comments.		See comments NASCIO-1 through NASCIO-8.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NASCIO-1	NASCIO	Chad Grant / Doug Robinson					Support for the emphasis on a Chain of Trust that allows updating and re-issuance of credentials based on the re-use of the identity registration process by establishing and authoritative enterprise identity store that is strongly bound to the individual. I. This coincides with best practice for information technology (IT) organizations and credentialing organizations. By focusing on the registration of identities organizations can create a re-usable identity, infrastructure for state employees, contractors and citizens. This is consistent with the States Identity, Credentialing and Access Management (SICAM) framework that closely follows those activities of the federal government. II. This supports enterprise IT identity management activity and streamlines provisioning and de-provisioning of enterprise applications. III. Establishing an authoritative data store which has proper access controls and security controls helps to ensure privacy and the protection of personally identifiable information (PII). As more and more states have laws covering PII, user control over PII and identity breach notification the best practice that results from a focus on a chain of trust brings multiple benefits to states and the CIOs.		Noted.
NASCIO-2	NASCIO	Chad Grant / Doug Robinson					Need to explicitly recognize Personal Identity Verification Interoperability (PIV-I) and specify where PIV-I does and does not comply with a Personal Identity Verification (PIV) standard and to clarify and delineate PIV and PIV-I requirements. I. Non-federal entities cannot do all of the items identified in FIPS-201. Non-federal entities choosing to adopt PIV-I within their architectures currently rely upon multiple federal documents and guidelines to understand PIV-I requirements. It is essential for the states and the federal government to be clear on requirements so relying parties have a clear understanding and trust of PIV-I issued credentials. II. For the items in FIPS-201 that non-federal entities cannot perform, whether technical, administrative, or policy – the needed clarification should support consistency and trust between non-federal, PIV-I issuing parties. III. PIV-C has added much confusion to interoperability discussions. If PIV-C is intended to be a different class of identity credential, then it should be rebranded as such and not confused with or included in PIV and PIV-I interoperable credentials and supporting standards and supplemental guidance.		Out of scope. The Identity, Credential and Access Management (ICAM) Subcommittee of the Federal CIO Council is responsible for PIV-I.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NASCIO-3	NASCIO	Chad Grant / Doug Robinson					Need for the specification to be form factor agnostic, allowing the use of mobile devices and other form factors in addition to the smart card form factor. It is important to get the concept of additional form factors included in FIPS 201-2 that will emulate PIV and PIV-I. I. It is crucial that NASCIO members have cost effective options for additional digital identity platforms. States must be prepared to respond to the growing adoption of mobile devices and services with appropriate authentication services. Currently, both the state workforce and citizens display a tremendous appetite for mobile-enabled applications. In order to serve these constituents, technologies that leverage secure identity elements in smart phones are crucial. Technology exists in Subscriber Identity Modules (SIMs) and in Micro Secure Digital (Micro SD) elements to achieve this. Further work needs to be done on binding individuals to these secure elements and also working with telecommunications providers to enable personal as well as subscriber identity to be enabled. By adopting a form factor agnostic approach devices of all kinds are more easily enabled. The benefits include cost saving, ease of use and increased flexibility to address multiple applications due to the capabilities of the smart phone platform.		Declined. FIPS 201-2 will specify the ability to create derived credentials from the PIV Card, but the PIV Card itself will remain as a smart card form factor. This does not, however, preclude the ICAMSC from making PIV-I form factor agnostic.
NASCIO-4	NASCIO	Chad Grant / Doug Robinson					Need for a standard on flexible and secure contactless communications enabling applications outside of logical access control such as physical access, payments, and parking. I. One area in which FIPS 201 is lacking is in the area of establishing a secure communications channel between the card and the reader in contactless modes of operation. Establishing standards for mutual authentication, secure channels and related secure contactless communication protocols will help the standard's applicability to as wide a range of use cases as possible and in doing so help with the economic justification for the investment in the infrastructure, credentials and applications to support it both by states as well as by industry.		Noted. The standard for secure channel will be specified in SP 800-73.
NASCIO-5	NASCIO	Chad Grant / Doug Robinson					Support for leveraging national and international standards such as those used for authentication services (ISO 24723), key management (Global Platform) and public key infrastructure (IETF RFC 5280, 2560 and 5055) among others.		Noted. FIPS 201 leverages national and international standards, where possible.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NASCIO-6	NASCIO	Chad Grant / Doug Robinson					Need to address the specific requirements for PIV-I including: option to expand the life of certificates out to 6 years to coincide with card life to address administrative and total costs and for the development of standards on background investigation for higher assurance levels. I. Given current budget environments NIST needs to recognize the need for states to have the flexibility to develop their own policy on certificate and PIV-I expiration. NASCIO would like to join NIST in engaging with the Federal Bridge Certificate Authority and its Management Authority in developing profiles that meet the need of states. Profiles which allow mapping to threats are a basic tenet of security system design. NASCIO recommends pursuing this flexibility to those states interested in pursuing PIV-I.		Out-of-Scope. The Identity, Credential and Access Management (ICAM) Subcommittee of the Federal CIO Council is responsible for PIV-I, and the Federal PKI Policy Authority is responsible for the Federal Bridge Certification Authority Certificate Policy, which specifies the maximum lifetimes for PIV-I certificates.
NASCIO-7	NASCIO	Chad Grant / Doug Robinson					Desire to have Special Publications (as opposed to the specific FIPS 201 provisions) handle technical details where flexibility is required due to technology lifecycles and changes in solutions in the marketplace. I. The current five year review cycle for FIPS 201 does not map well to the technology lifecycle of many of the components in identity, credentialing and access control systems. By moving items such as authentication factors to a Special Publication (normative) NIST can improve the applicability of FIPS 201 with regards to the solutions available in the marketplace.		Noted. The FIPS 201 editing team is continuously using the suggested approach in regard to moving technical details to relevant NIST Special Publications.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NASCIO-8	NASCIO	Chad Grant / Doug Robinson					Desire to mature and leverage common trusted infrastructure to electronically authenticate credential validity, ensure intended user, and enable use of electronic exchange and digital signature. Biometric "match on card" (or any other form factor) to ensure that the intended individual is the individual is desired, should be encouraged, and potentially be made mandatory in the future. However, additional standards, efforts, and activities may be required to increase confidence. I. States have a number of use cases with the potential of significant return on investment (ROI) by using the digital infrastructure to conduct transactions in the future -- in particular digital signatures. Digital signatures make process demands on the end-users including: (A) they are aware that they are signing by such action, (B) increase the awareness and consequences of such action, and (C) that there is proof that it is the intended user that is signing. The last part brings the need for biometric match on card (or other form factor) to prove that it is truly that individual that provided the signing. This provides greater assurance than the use of PIN for proof of A, B and C above and to provide non-repudiation. II. States are concerned that current framing and standards are limiting from a broader community implementation perspective, and that if done now, may require future significant infrastructure changes to resolve. III. Federal and private-sector efforts to mature standards, implementation experience and gain community confidence of costs and risks is encouraged.		Noted.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NCE-0	NCE	T.K. Gaines	G	-	-	-	Options for incorporating Alternate Form Factors Credentials into business processes should be addressed by FIPS 201-2.	As per multi-agency discussions with NIST it is recommended that NIST: 1) Write FIPS 201-2 to accommodate development and use of alternate form factor credentials "in general" – leaving it up to a SP to define the details &/or limits. 2) Consider the potential of emerging technologies and the ability to authorize non-PIV devices by an explicit action of a PIV cardholder to establish a trusted work session. (e.g., use of a PIV Card at the user desktop to "activate" a tablet or smart phone with your identity for one day, a week, a month, etc.). [Note: A number of agency experts believe that if the federal government's efforts do not deliberately make provision for alternate form factors and alternate work processes, COTS space products may well overwhelm the worspace in lieu of the PIV card instead of operating in conjunction with the PIV card.]	Resolved by DOT-21.
NCE-1	NCE	T.K. Gaines	G	vi	169	Fwd Para 9	Text reads, "This standard is effective immediately."	Adoption/migration/implementation time needs to be taken into account. • "each adoption/migration target should be addressed by a separate focused activity organized within an ICAMSC working group; • Participation in the activity should be open to all interested government parties (employees and active contractors)" Example targets include: • Issuer migration/adoption • LACS migration/adoption • PACS migration/adoption • Iris enrollment/issuer-use migration	Resolved by DoD-3.
NCE-2	NCE	T.K. Gaines	T	5	360 - 361	2.1	The specifics of how the NACI indicator requirement will be handled and monitored is unclear. While a NACI may be initiated it is not necessarily completed and even when it is completed the CMS/record data is not necessarily updated.	In addition to specifying where and how the NACI is to be indicated, clarify the agency requirements for documenting and updating the status.	Resolved by OPM-3.
NCE-3	NCE	T.K. Gaines	T	5 & 8		2.1 & 2.4	The requirement for favorable adjudication is not clearly stated. The current wording only stipulates the initiation of a NACI or equivalent or locating a prior one that has been successfully adjudicated. With respect to the NCHC the words are "completed before issuing . . ." and the text only mentions the results of "the investigation."	Clearly specify: 1) the minimum requirement for PIV credential issuance is favorable adjudication of an NCHC; 2) the requirement for the NACI be completed and favorably adjudicated; and 3) the required actions if either adjudication is unfavorable.	Declined. Current language is consistent with the Springer Memorandum and M-05-24.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NCE-4	NCE	T.K. Gaines	T	6		2.3	Section does not currently recognize/use biometric data that is available on some foreign passports.	Consider the possibility of capturing biometric data from foreign (other?) passports if available.	Declined. The infrastructure needed to read and check the certificate on all e-passports is non-existent in PIV issuance processes.
NCE-5	NCE	T.K. Gaines	T	6		2.3	Without a legitimate method of verifying the validity of identity source documents, the identity proofing process cannot attain the goals set out for PIV. (This is especially true if there is no background investigation associated with the issuance specifically in the case of a PIV-I credential.)	The method of establishing the validity and authenticity of identity source documents needs to be clearly specified either in FIPS 201 or an associated special publication.	Noted. PIV-I is not in scope for this Standard.
NCE-6	NCE	T.K. Gaines	T	6	391 - 393	2.3	The new draft tiered investigation requirements document "FEDERAL INVESTIGATIVE STANDARDS" from OPM establishes it as an agency responsibility to confirm the subjects POB & DOB. One of the documents that can be used for this purpose is a U.S. passport either valid or expired. If OPM allows the use of an expired passport why should FIPS exclude it for PIV purposes?	1. Resolve the conflict between the draft NIST and OPM documents and update FIPS 201-2 as/if appropriate. 2. Stipulate in FIPS 201-2 that confirmation of POB and DOB occur at the time of enrollment.	1) Declined. FIPS 201 identity proofing requirement are derived from I-9 form, which requires unexpired ID source documents. 2) Declined. POB and DOB confirmation is not part of FIPS 201 identity proofing and registration requirements.
NCE-7	NCE	T.K. Gaines	T	6	410	2.3	Why is the DoD CAC singled out in the list of primary identification documents?	It seems the text should either encompass all agency PIV credentials or none.	Resolved by replacing the Common Access Card with the PIV Card on the list.
NCE-8	NCE	T.K. Gaines	T	7	411 - 437	2.3	In the secondary identity source document section, do not attempt to specify which documents may not be expired or canceled. We don't necessarily know in each case and this could change over time.	Instead of specifying which documents may not be expired or canceled, consider using the following wording in the lead in paragraph: "The secondary identity source document (neither expired or canceled where applicable) may also be any of the following:"	Resolved by changing line 392 to include secondary source document. Changed "The primary identity source document shall be neither expired nor cancelled" to "The identity source documents shall be bound to that applicant and shall be neither expired nor cancelled." Also, removed 'unexpired' from the listed documents in secondary source documents.
NCE-9	NCE	T.K. Gaines	G	multiple	multiple	2.4 and other	Iris imaging & use capability will take some time to implement.	The FIPS 201-2 adoption/migration process specified will need to make allowance for some significant transition time.	Noted. In the revised draft, support for the iris biometric is optional.
NCE-10	NCE	T.K. Gaines	T	8	457 - 460	2.4	The last sentence needs to be clarified.	Recommend the following wording: "If the PIV credential is issued based on a satisfactorily adjudicated NCHC, the PIV credential shall be revoked if the NACI or equivalent adjudication so justifies."	Resolved by revising the paragraph as per OPM-3. Note: According to OPM, NCHC is not adjudicated - only NACI is adjudicated. Revocation of credential is addressed by the last statement of the section.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NCE-11	NCE	T.K. Gaines	T	8	465 - 469	2.4	Is iris imaging truly our best alternative? Should there be any allowance for other alternate biometrics? Is it possible to move most if not all of the alternate biometric specifics to an appropriate Special Publication to assure that this can be modified in a timely manner as needed? How are iris scan images supposed to be used by OPM to facilitate background investigations? e.g., they are not captured at bookings, people don't leave them behind a crime scenes, etc.	Recognizing that a near universal approach is necessary for effectiveness, please confirm/specify rationale for iris. Consider placing most if not all technical requirements and details in the SP. Specify that the only purpose for capturing iris scan images is to facilitate identity verification. They are not intended to support the background investigation (NCHC or NACI) process.	Overcome - iris and face are now optional see DOT-11 and NCE-37. Noted. See DOT-8.
NCE-12	NCE	T.K. Gaines	G	8	474	2.4	The text reads, ". . . not considered PIV Issued Cards." This is the first and only time the expression/term "PIV Issued Cards" is used.	Provide clarification of the expression. Adding the term to the glossary may be sufficient.	Resolved by Cert-18.
NCE-13	NCE	T.K. Gaines	T	8 & 9	478 - 489	2.4.1	Pseudonyms	Clarify the following: - the enrollment expectations - expectation for identity source documents, if any, for such individuals - what information is expected to be shared between agencies, - etc. Address the impact pseudonyms may have on the chain of trust. Clarify the expectations for enrollment officers/registrars and activators who are involved with these records regarding protection/knowledge of their true identity.	Resolved by DOT-14 and revised text.
NCE-14	NCE	T.K. Gaines	T	9	491 - 494	2.4.2	Contrary to the fereral register notice, it is not clear what is required for new PIV card issuance within grace period cases. The text merely states that a new PIV Card may be issued in a manner consistent with PIV Card Issuance. From this some could interpret that full enrollment is required along with an NCHC and a NACI (including favorable adjudication for both). Also, according the federal register notice, a new NCHC is required. Why? If it is required, does it require a new set of prints? If so, there is no real benefit from "relaxing the requirements." The same number of enrollment station visits may be required and little if any time savings will be realized.	1) Clearly specify the difference in the issuance requirements between new issuance and re-issuance within the approved interregnum. 2) Clarify why is a new NCHC required. Is it to be required if it has only been a day, two days, three, between agencies/employments? If employment is unbroken and no additional NCHC is required, why does a few days of broken service necessitiate a new NCHC. - Note: if new fingerprints are to be captured for the NCHC, another visit to the enrollment station will be required so 2 visits will still be required to obtain a new credential. (1 for enrollment & 1 for card pick-up and activation). Are there different expectations?	1) Resolved by Cert-20. 2) Per OPM/OMB feedback, NCHC is not a requirement.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NCE-15	NCE	T.K. Gaines	T	9	494	2.4.2	The language used here does not adequately clarify the process for a managed service operating with card issuance/re-issuance terminology. The text needs to make a clear distinction between re-issuance (requires re-enrollment) and reprint (does not require re-enrollment)	Clarify the terminology and include the terms in the E.1 Glossary of Terms. Re-issuance - includes what is called re-print by some. Also, establish that replacing lost/stolen credentials does not require re-enrollment by specifically providing for the 1:1 biometric match at the time of activation.	Decline to define the terms in glossary. Reprint does not appear in FIPS 201. Reissuance in FIPS 201 does not require re-enrollment with the new chain-of-trust concept.
NCE-16	NCE	T.K. Gaines	T	9	506 - 526	2.5.1	Contrary to the fereral register notice, this section does not go far enough address/resolve the ambiguity of terms and usage surrounding terms such as re-issue, reprint, renewal, etc.	Clarify the expectations and the differences provided for between the various card actions. Specifically include or address the term reprint, in the glossary or both.	Resolved by NCE-15.
NCE-17	NCE	T.K. Gaines	T	9	510 - 511	2.5.1	4th sentence (& 2.5.2 second paragraph): It is unclear exactly what is expected of whom here.	How is this check to be signified and enforced? What is to keep the role holder from requesting the card renewal without completing a minimal verification of "good standing" and personnel records status?	Declined. See SP 800-79-1, AI13 control.
NCE-18	NCE	T.K. Gaines	T	9	511 - 512	2.5.1	5th sentence: Is it the expectation that OPM will start requiring periodic re-investigation for those issued a PIV card?	Currently there is no such requirement for the PIV card itself. Implementing such a requirement will have a significant impact on the cost of HSPD-12 implementation.	See OPM-4. (This text has been coordinated with OPM.)
NCE-19	NCE	T.K. Gaines	T	9	512 - 513	2.5.1	6th sentence: Is the biometric match expected at the time of request or only at the time of activation?	Clarify the expectation here. Also, specify the expectation and/or reference to be followed if neither form of biometric match is available/possible.	A successful one-to-one match is required at the time of issuance. See new text in Section 2.9.1. Resolved by DOT-18.
NCE-20	NCE	T.K. Gaines		9	517	2.5.1	2nd paragraph: there is some degree of consensus among agencies that a 12 week window is not adequate to support effective management of the card renewal process.	Provide for up to and including 180 days as the standard card renewal window.	Resolved by DHS-4.
NCE-21	NCE	T.K. Gaines	T	9 - 10		2.5 - 2.5.2	In the case of lost or stolen credentials it needs to be clear that the chain of trust can be re-established at the time of activation instead of requiring re-enrollment?	Specifically spell out the ability to re-establish chain of trust at the time of activation.	Declined. Reconnecting to the chain-of-trust is possible at renewal and reissuance.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NCE-22	NCE	T.K. Gaines	T	9 & 10		2.5.1	PIV Card Renewal & 2.5.2 Reissuance	The renewal process needs to provide for maintaining and using the 'old' card until the new card arrives and is activated. We do not need additional instances in which personnel are expected to function without an active PIV card. Recommend revising the text to read, "The original/current PIV Card must be surrendered prior to the issuance/activation of the new PIV Card." Note: Lost or stolen credentials are a straightforward reissuance case, but damaged cards may still provide some functionality while the new card is being produced.	Resolved by DOJ-4.
NCE-23	NCE	T.K. Gaines	T	10	524 - 525	2.5.1	3rd paragraph: Up to 12 years between capture of biometric and photo information, may be way too long for most people if the biometrics and photo are expected to be a reasonable representation of their current information.	If the expectation is that agency identity and/or card management will effect necessary updates to biometrics and photos, please state this clearly. Otherwise, it seems that 12 year timeframe is excessive.	Resolved by Cert-30.
NCE-24	NCE	T.K. Gaines	T	10	557	2.5.2	4th paragraph: Collection & destruction of the PIV card for lost or stolen is typically not applicable in "lost or stolen" cases and there are cases where a "damaged" PIV card may provide some functionality and collection/destruction should be allowed to occur at the time of new card issuance/activation.	Modify the words to provide for card collection and destruction at the time of new card issuance/activation.	Resolved by replacing: "If the card cannot be collected, normal operational procedures shall be completed within 18 hours of notification." with: "In the case of a lost, stolen or compromised card, normal revocation procedures shall be completed within 18 hours of notification."
NCE-25	NCE	T.K. Gaines	T	11	577 - 579	2.5.3	In cases of compromise it would seem that the certificates should be terminated immediately with rekey to follow as soon as possible. Yet, some implementations of the card management system require and enforce card termination if the certificates are terminated. So it would not be possible to rekey and then reuse the card under those conditions.	It is important to establish that card termination is not required in such cases even though the certificates may be terminated. However, it is not clear to all that such a policy is consistent with common policy so this too may require some clarification.	Noted.
NCE-26	NCE	T.K. Gaines	T	11	596 -598	2.5.4	2nd paragraph, 4th bullet: Provision should be made for recovery effort, prior to card termination.	Specifically USAccess has some ability to recover/retry card updates. If this can be done with compromise of the system or the card, it should be allowed prior requiring card termination.	Resolved by DoD-27.
NCE-27	NCE	T.K. Gaines	T	11	616 - 617	2.5.5	While the intended meaining of the text appears to be decipherable, it may be confusing to many and it seems to suggest there is always an alternate biometric available for matching purposes.	Clarify the wording and explain how it is supposed to provide for a meaningful option when there is effectively no alternate biometric available. In certain use cases it may help to require biometric authentication to the chain of trust prior to reset.	Resolved by GSA-17.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NCE-28	NCE	T.K. Gaines	T	12 - 13	622 - 645	2.5.6	The expectation for timeliness of termination is not specified.	Clarify what is expected. Use of the term "immediately terminate" may be appropriate but, will still need to recognize that some time may be required and circumstances may preclude "immediate" termination.	Resolved by AMAG-5.
NCE-29	NCE	T.K. Gaines	T	12 - 13	622 - 645	2.5.6	The text needs to clearly specify that certificate expiration either is/is not cause for revoking the credential.	If the credential is in fact to be revoked upon certificate expiration, the text should specify that confiscation of the revoked credential is the expected action if the credential is presented for identity verification purposes. (Note: some grace period may be appropriate.) If a grace period is deemed appropriate, the limit of the grace period should be established.	Section 5.5 already says “The presence of a valid, unexpired, and unrevoked authentication certificate on a card is proof that the card was issued and is not revoked.” An expired certificate cannot be revoked. This section, which only addresses circumstances in which the cardholder is no longer eligible to have a PIV Card (see Cert-42), already requires the PIV Card to be collected and destroyed if possible (as do the sections on reissuance and renewal).
NCE-30	NCE	T.K. Gaines	T	12 & 13	637 - 638	2.5.6	Wording establishes that departments/agencies may revoke digital signature and key management keys. Why is this optional? Current practices, at least in the GSA MSO, revokes all certificates.	Either clarify the reasoning or change the text to require revocation of all certificates.	Resolved by GSA-18.
NCE-31	NCE	T.K. Gaines	E	13	639	2.5.6	Text reads, "CRLs issued shall include the appropriate certificate serial numbers."	Recommend that "appropriate" be replaced with "revoked"	Resolved by removing details on how to perform revocation.
NCE-32	NCE	Lozano	E	13	643	2.5.6	The acronym "IIF" is used without explanation.	Recommend defining the IIF acronym upon first use even though it is in the glossary.	Accept use of PII. All instances of IIF will be replaced by PII. We will define PII with a reference to OMB M-07-16. Also, delete IIF from the glossary.
NCE-33	NCE	T.K. Gaines	T	21	893 - 896	4.1.3	It could be difficult to ensure compliance with the "blanket" first sentence - either now or later. Also, the raised lamination on the card face as well as the absence of lamination in the area of the chip could provide the desired orientation indication.	Consider more careful wording of the first sentence to recognize there may be limits to what can be reasonably done with a smart card.	Resolved by DoD-32.
NCE-34	NCE	T.K. Gaines	T	22	901 - 909	4.1.3	Punching holes in the card could cause unintended damage for any number of reasons and warranty coverage my still be compromised. It may be best to exclude this as an option.	Other options should be exhausted prior to this one being used. (e.g., a padded pressure clip) If hole punching were to be chosen, the method and/or tools used for punching the hole would need to be established and verified, the decision officially documented along with the manufacturers approval. Further, additional product testing would likely be required. (see comment below)	Declined. FIPS 201-2 already describes how this can be done safely.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NCE-35	NCE	T.K. Gaines	E	22	915	4.1.3	As written, it seems this line could be left over from the drafting process.	Either delete the line or expand on the thought and make it a note. e.g., "Note: Additional PIV Card testing may be required to assure that modifications designed to assist with 508 compliance have not compromised the card function." Yet even with this clarification and additional information that may be needed, it could be unnecessary to cover this in FIPS 201 and it may be better address the concern in the appropriate SP.	Resolved by AI-4 and ES-10.
NCE-36	NCE	T.K. Gaines	T	23		4.1.4.1	Full Last Name and Full First Name need to remain a requirement. Either, full Middle name(s) or Middile initial(s) should be an option. Prefixes are rarely essential. Suffixes and multiple middle/last name elements must be accommodated both on the chip and on the printed card face. The sequence of names (Last, First, Middle) must be consistent and it must be clear, on the chip and in the printed text, which name(s) belong with which portion of the name (first, middle or last). Finally, the suffix, if any, must follow immediately after the Last name.	Request the text and graphics be adjusted accordingly.	- Decline to make middle name optional. Added examples in Table 4-1 that shows either full middle name or middle initial is required, if present. - Suffixes and multiple middle / last name elements are already accommodated both on the chip and on the printed card face. - Decline to make Suffix part of Primary Identifier. Suffix will be a part of secondary identifier as per ICAO 9303. - Decline to specify all name components. Given the large variations in names and cultural differences, it is not always possible to cleanly separate the first, middle, and last names.
NCE-37	NCE	T.K. Gaines	T	42	1316 - 1327	4.4	The text need to be more clear. The first bullet does not appear to accurately address the iris option/ requirement. Further, the facial image should be stored on the card. Many rely on this feature for a quick check of card validity that provides for some local, although not definitive, authentication of card and its presenter.	The text needs to recognize: fingerprints may not be available; either fingerprints or the iris is required if available; if neither is available, the text needs to specify how the record is to be processed. Make it a requirement to have the facial image stored on the card and only accessible through use of the PIN.	Resolved by stating that iris is optional and storage of facial image on the PIV Card is mandatory. Moreover, clarification of how the record is to be processed will be provided as follows: On line 1323 replace "If no fingerprints can be collected, two electronic iris images shall be stored on the PIV Card." with "If no fingerprint images meeting the quality criteria of [SP 800-76] are available, the PIV Card shall nevertheless be populated with fingerprint records as specified in [SP800-76]". And position this text into the new Section 4 (on PIV data model) as appropriate. This practice will appear in SP 800-76-2. It implements the treatment of missing fingerprint data established in idmanagement.gov guidance document http://www.idmanagement.gov/documents/NISTPIVfingerprintExceptionHandlingGuidelines.pdf.
NCE-38	NCE	T.K. Gaines	T	42	1338	4.4.1	The text appears to indicate the need/requirement to import fingerprints obtained from sources other than the service enrollment station for incorporation into the CMS. At present, as I understand it, there is no such capability within USAccess, the GSA managed service.	Clarify the expectation here. This may well be perceived as a new requirement and another one which may take some time to implement. Alternatively, if the only expectation is that OPM will receive the paper fingerprint card, the process could be more simple. However, if fingerprints are obtained via an outside source there need to be some clear chain of custody requirements. The applicant should never have custody of their own fingerprint cards.	Resolved by DoD-2 and WM-24.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NCE-39	NCE	T.K. Gaines	T	43	N/A	Footnote 13 or 14	The value/meaning of "creating a new chain of trust" is unclear in cases where no fingerprint or iris images are available. Also the text speaks of "implying" a new NCHC.	Clarify the expectation and establish whether a new NCHC is required or not. Also, would a full or only a partial "enrollment" be expected. i.e., possibly bio update only?	Resolved by DoD-54.
NCE-40	NCE	Lozano	E	46	1479	4.5.2	Third sentence addresses "contact" readers, but this section header deals with "Contactless Reader Requirements."	Change "contact" to "contactless. Ensure the referenced SP is still applicable.	Resolved by AMAG-10.
NCE-41	NCE	Lozano	E	49	1548	5.4	The acronym "OIDs" is used without explanation.	Recommend defining the OID acronym upon first use even though it is in the glossary.	Accept.
NCE-42	NCE	Lozano	E	49	1566	5.5	The acronym LDAP is used without definition.	Recommend defining the LDAP acronym upon first use even though it is in the glossary.	Accept.
NCE-43	NCE	Lozano	E	57	1800	5.5	The typographical error "aIf" needs to be corrected.	"aIf" should be "if"	Accept.
NCE-44	NCE	T.K. Gaines	T	61	1924 - 1932	A.5	Product testing must go beyond initial function. Endurance and potential for unintended consequence of repeated use must also be considered & addressed. Approved products have been found to damage cards and/or cause card failure over time.	Either in 201 or in an SP - stipulate additional demands and rigor in the product testing.	Declined. GSA EP is the authority for additional product testing.
NGA-1	National Gallery of Art	Nabil Ghadiali	E	iii and 3	79, 307	ABSTRACT and 1.4	The requirements for the accreditation of the PIV Card issuer are specified in the Special Publication 800-79, Guidelines for the Accreditation of Personal Identity Verification Card Issuers (PCI's).	Removed apostrophe from PCI's - The requirements for the accreditation of the PIV Card issuer are specified in the Special Publication 800-79, Guidelines for the Accreditation of Personal Identity Verification Card Issuers **(PCIs).**	Resolved by deleting "(PCI's)" from Abstract and from Section 1.4.
NGA-2	National Gallery of Art	Nabil Ghadiali	G	v	155	8	Clarify the definition of a PIV Card in the document and not only in the glossary of terms.	Clarify that a PIV Card is one that is personalized for a Federal Employee or a Contractor. Blank Cards are not PIV Cards. This is because several durability requirements apply to personalized PV Cards and not blank card stock.	Declined. The PIV Card should not be defined around test requirements. The current definition is accurate and does not need to be repeated.
NGA-3	National Gallery of Art	Nabil Ghadiali	T	6	384	2.3	The organization shall adopt and use an approved identity proofing and registration process in accordance with [SP 800-79].	Identity proofing and registration requirements are not outlined in SP 800-79. SP 800-79 does not provide any new requirements. Identity proofing and registration requirements are to be specified in Section 2.3. Recommend deleting this bullet.	Declined. The sentence is appropriate, since SP 800-79 specifies the approval and adoption requirements for FIPS 201 identity proofing, registration, and issuance processes.
NGA-4	National Gallery of Art	Nabil Ghadiali	T	8	450	2.4	Several requirements from Section 2.3 are repeated.	Recommend combining Section 2.3 and 2.4 titled - PIV Card Identity Proofing, Registration and Issuance Requirements.	Declined. The responsible parties are different and so the process is different.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NGA-5	National Gallery of Art	Nabil Ghadiali	T	8	455	2.4	The organization shall use an approved PIV credential issuance process in accordance with [SP 800-79].	Issuance requirements are not outlined in SP 800-79. SP 800-79 does not provide any new requirements. Issuance requirements are to be specified in Section 2.4. Recommend deleting this bullet.	Declined. This bullet requires compliance with SP 800-79. SP 800-79 provides approval process for the issuance requirements outlined in this bullet.
NGA-6	National Gallery of Art	Nabil Ghadiali	T	8	470	2.4	The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited).	Recommend that this sentence be reworded to include SP 800-79 in it. The organization shall issue PIV credentials only through systems and providers who have been accredited in accordance to SP 800-79.	Resolved by adding reference to SP 800-79 in the current text.
NGA-7	National Gallery of Art	Nabil Ghadiali	T	9	486	2.4.1	The issuance of a PIV Card using a pseudonym shall follow the procedures in PIV Card Issuance Requirements for employee name changes except that the employee must provide evidence satisfactory to the card issuer that the pseudonym is authorized by the employee's agency.	Wouldn't the employee agency know of its own policies? If so why would the employee need to provide proof to the card issuer.	Resolved by new text.
NGA-8	National Gallery of Art	Nabil Ghadiali	T	10	524	2.5.1	The same biometric data may be reused with the new PIV Card if the expiration date of the new PIV Card is no later than twelve years after the date that the biometric data was obtained.	Where is the date of issue of the biometric stored? How is the 12 years computed? Is the expiration date of the biometric in the CBEFF header? If yes, please clarify.	Resolved by NGA-12.
NGA-9	National Gallery of Art	Nabil Ghadiali	T	10	533	2.5.2	A cardholder shall apply for reissuance of a new PIV Card if the old PIV Card has been compromised, lost, stolen, or damaged.	Reissuance also applies when the renewal period of 12 weeks is over.	Resolved by DOT-15.
NGA-10	National Gallery of Art	Nabil Ghadiali	T	10	544	2.5.2	When reissuing a PIV Card, normal operational procedures must be in place to ensure the following: …..	If reissuance also applies when the renewal period is over, then the 3 bullets that follow the sentence (When reissuing a PIV Card, normal operational procedures must be in place to ensure the following:) may not apply.	Resolved by DOT-15.
NGA-11	National Gallery of Art	Nabil Ghadiali	T	10	548	2.5.2	Revocation of the Digital Signature Key certificate is only optional if the PIV Card has been collected and zeroized or destroyed.	Revocation of the Digital Signature Key certificate is only optional if the PIV Card has **<u>NOT</u>** been collected and zeroized or destroyed. If the card is collected and destroyed, then revocation may not be necessary on a reissued card.	Resolved by DOT-15.
NGA-12	National Gallery of Art	Nabil Ghadiali	T	11	564	2.5.2	The same biometric data may be reused with the new PIV Card if the expiration date of the new PIV Card is no later than twelve years after the date that the biometric data was obtained.	Please clarify how the 12 years is to be computed. Where is the issuance or expiry date of the biometric stored? Is in in the CBEFF Header of the biometric?	Noted. The date of collection is encoded in the creation date entry of the CBEFF header as specified in [SP 800-76]. This date may be used to compute the time elapsed since a biometric was collected.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NGA-13	National Gallery of Art	Nabil Ghadiali	T	11	569	2.5.2.1	In the event that a cardholder notifies a card issuer that his or her name has changed, and presents the card issuer with evidence of a formal name change, such as a marriage certificate, a divorce decree, judicial recognition of a name change, or other mechanism permitted by State law or regulation, the card issuer shall issue the cardholder a new card following the procedures set out in Section 2.5.2, PIV Card Reissuance.	Suggest that the cardholder provide the same list of documents stated in Section 2.3 to prove name change and not marriage certificate, divorce decree or any other document.	Declined. This text does not preclude identity source document as evidence of name change.
NGA-14	National Gallery of Art	Nabil Ghadiali	T	11	582	2.5.4	The Post Issuance update applies to cases where one or more certificates, keys, biometric data objects, or signed data objects are updated. The PIV Card expiration date or the FASC-N shall not be modified by a Post Issuance update	Please add that the Printed Information Buffer may not be updated as well.	Resolved by NIST-95. SP 800-73 will address this.
NGA-15	National Gallery of Art	Nabil Ghadiali	E	11	596	2.5.4	If the PIV Card post issuance update begins but fails for any reason, the PIV Card issuer shall immediately terminate the PIV Card as described in Section 2.5.6, and a diligent attempt shall be made to collect and destroy the PIV Card.	Recommend adding - "in the event a compromise is suspected" to the end of the sentence. If the PIV Card post issuance update begins2 but fails for any reason, the PIV Card issuer shall immediately terminate the PIV Card as described in Section 2.5.6, and a diligent attempt shall be made to collect and destroy the PIV Card in the event a compromise is suspected.	Resolved by DoD-27.
NGA-16	National Gallery of Art	Nabil Ghadiali	E	13	661	2.6	The Senior Agency Official for Privacy…..	Recommend using "Privacy Official" to match with the SP 800-79-1 role.	Resolved by accepting the change and adding a following footnote explaining the change: Privacy Official refers to the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO).
NGA-17	National Gallery of Art	Nabil Ghadiali	T	21	895	4.1.3	One method is adherence of a raised surface (for example, an adhesive Braille letter). Section 4.1.4.3 defines Zone 21F, where raised surface may be placed.	Please indicate whether this raised surface is subject to the ANSI 322 durability tests or not.	Resolved by removing the example.
NGA-18	National Gallery of Art	Nabil Ghadiali	E	22	915	4.1.3	The PIV Card may be subjected to additional testing.	Sentence doesn't provide a context as written. Possible rewording - "*The PIV Card may be subjected to additional testing as per the Dept or Agency requirements*".	Resolved by AI-4 and ES-10.
NGA-19	National Gallery of Art	Nabil Ghadiali	E	23	943	4.1.4.1	The full name shall be printed directly under the photograph in capital letters. The full name shall be composed of a Primary Identifier (i.e., surnames or family names) and a Secondary Identifier (i.e., pre-names or given names)	Please add that the printed name shall match that mentioned in the Identity Source document to the extent possible to remove any ambiguity.	Resolved by adding the following sentence: "The printed name shall match the name on the identity source documents provided during identity proofing and registration to the extent possible."
NGA-20	National Gallery of Art	Nabil Ghadiali	T	29, 30, 31, 32	1075, 1080, 1083, 1088	Figure 4-2, Figure 4-3, Figure 4-4, Figure 4-5	In Zone 2F- Name, please show the name as indicated in Table 4-1 and not only JOHN DOE.		Declined. JOHN DOE is a non-private and non-invasive way to show examples.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NGA-21	National Gallery of Art	Nabil Ghadiali	T	38	1165	4.1.7.1	The PIV Card shall include mechanisms to block activation of the card after a number of consecutive failed activation attempts.	Please add that the number of consecutive failed attempts is left up to the Agency to decide.	Declined. This is already stated in Section 2.5.5 (now Section 2.9.4) as follows: The Personal Identification Number (PIN) on a PIV Card may need to be reset if the cardholder has forgotten the PIN or if PIN-based cardholder authentication has been disabled from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency.
NGA-22	National Gallery of Art	Nabil Ghadiali	T	38	1186	4.2	It is strongly recommended that a complete CHUID should not be stored in relying systems.	Please add - if the entire CHUID is stored, it should be stored in a hashed format such that it cannot be extracted and used.	Resolved by removing the third paragraph of section 4.2 (now Section 4.2.1), lines 1184-1187. See ICAMSC-89.
NGA-23	National Gallery of Art	Nabil Ghadiali	T	39	1187	5.2	It is strongly recommended that a complete CHUID should not be stored in relying systems.	Please add - if the entire CHUID is stored, it should be stored in a hashed format such that it cannot be extracted and used.	Resolved by NGA-22.
NGA-24	National Gallery of Art	Nabil Ghadiali	T	40	1235	4.3	Where digital signature keys are supported, the PIV Card is not required to implement a secure hash algorithm. Message hashing may be performed off card	Suggest deleting these two sentences. SP 800-78 does not mention any hashing algorithms that can be implemented by the card. Hashing is performed off the card, due to lack of specifications in SP 800-73 and SP 800-78.	Accept.
NGA-25	National Gallery of Art	Nabil Ghadiali	T	40	1245	4.3	The PIV authentication key shall be an asymmetric private key that is accessible from the contact interface and supports card authentication for an interoperable environment. This is a mandatory key for each PIV Card.	The PIV authentication key shall be an asymmetric private key that is accessible from the contact interface and supports **cardholder** authentication for an interoperable environment. This is a mandatory key for each PIV Card. Suggest rewording this sentence to match CTE authentication where the asymmetric key is used to prove the cardholders identity to the external entity.	Resolved by DoD-43.
NGA-26	National Gallery of Art	Nabil Ghadiali	T	40	1258	4.3	The card management key is a symmetric key used for personalization and post-issuance activities, and it is optional.	Recommend that the card management key be made mandatory. This is because in Section 4.1.7.2 - Activation by Card Management System it states - "*When cards are personalized, card management keys shall be set to be specific to each PIV Card. That is, each PIV Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800- 78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP 800-78]*". This implies that card management keys are mandatory.	Declined. The lead-in sentence to Section 4.1.7.2 (now Section 4.3.2) clearly identifies the key as an optional key.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NGA-27	National Gallery of Art	Nabil Ghadiali	T	41	1290	4.3	The expiration date of the certificate must be no later than the expiration date of the PIV Card.	Can the expiration date of the certificates on the PIV Card be different from each other? Do the PIV Auth certificate and Card Auth certificate expirate dates need to be the same? Please clarify.	Decline to make changes in FIPS 201. Note that the expiration dates of PIV Authentication certificate and Card Authentication certificate do not need to be the same. And since the dates do not need to be the same, FIPS 201 does not need to state a non-requirement.
NGA-28	National Gallery of Art	Nabil Ghadiali	T	43	1349	4.4.1	The biometric data in the chain-of-trust shall be valid for at most 12 years.	Please clarify how the 12 years is to be computed.	Resolved by NGA-12.
NGA-29	National Gallery of Art	Nabil Ghadiali	E	44	1408	4.4.1	These fingerprint templates shall be used for 1:1 biometric verification against live samples collected from the PIV cardholder (see Section 6.2.3). Even though two fingerprints are available on the card, a department or agency has the option to use one or both of them for the purpose of PIV cardholder authentication. If only one fingerprint is used for authentication, then the primary finger shall be used first. In cases where there is difficulty in collecting even a single live scan sample fingerprint of acceptable quality, the department or agency shall perform authentication using asymmetric cryptography as described in Section 6.2.4.1	Iris matching is also a possibility in this situation. Please mention.	Resolved by deleting line 1408 -1414.
NGA-30	National Gallery of Art	Nabil Ghadiali	T	46	1459	4.4.3	The use of the electromagnetically opaque sleeve is removed from FIPS 201-2 altogether. This is no mention of a sleeve anywhere else in the document.	Please re-introduce the use of the electromagnetically opaque sleeve back into FIPS 201-2 in an appropriate section.	Declined. Sleeves were mentioned in Section 2.6 of the 2011 draft and also in the revised draft's Section 2.11.
NGA-31	National Gallery of Art	Nabil Ghadiali	E	48	1521	5.2	[COMMON] requires FIPS 140 Level 2 validation for the subscriber cryptographic module (i.e., the PIV Card). In addition, this standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.	Recommend deleting this paragraph from this section. The first sentence doesn't belong in this section and the second sentence is repeated. It has already been mentioned in Section 4.3	Resolved by deleting the first sentence of the paragraph and moving the second sentence to Section 4.2.2 (previously Section 4.3).
NGA-32	National Gallery of Art	Nabil Ghadiali	T	54	1702	6.2.3	Mention on-card-comparison as well for releasing of the PIV biometric.		Declined. There is a security and privacy risk in using OCC to read stored biometric data from the card. Cardholder activation via PIN entry is required to read the biometric.
NGA-33	National Gallery of Art	Nabil Ghadiali	T	56	1769	6.2.4.1	The Subject Distinguished Name (DN) and unique identifier from the authentication certificate are extracted and passed as input to the access control decision.	Suggest rewording to - "The FASC-N from the PIV authentication certificate is extracted and passed as input to the access control decision."	Resolved by NIST-81.
NGA-34	National Gallery of Art	Nabil Ghadiali	E	60	1888	A.2	Please revise heading and content to reflect new terminology from SP 800-37. It is now known as "security authorization" and not "certification and accreditation."		Resolved by new text.
NGA-35	National Gallery of Art	Nabil Ghadiali	E	63	1947	Appendix C	This table is confusing. Not sure what the "dots/bullets" are meant to represent.		Resolved by deleting Appendix C.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NGA-36	National Gallery of Art	Nabil Ghadiali	E	78	2355	Appendix G	Added an option to include country(ies) of citizenship of Foreign Nationals in the PIV Authentication Certificate.	Did not find this option in the document.	Resolved by deleting this text from the Revision History. Note: It is possible to include this information in PIV Authentication certificates, since [PROF] states: “Certificate and CRL issuers may include additional information in non-critical extensions for local use, but should not expect clients in the Federal PKI to process this additional information.”
NIST-1	NIST	William MacGregor	G			General	There are few cases where FIPS 201, or one of the SP's, requires behavior that is not conformant to ISO/IEC 7816 or 14443.	Recommend that FIPS 201 contain a "primacy" clause. Basically, this would say, "In the event inconsistencies between normative statements in FIPS 201-2, normatively referenced NIST publications, and normatively referenced standards of other origin, statements contained entirely within FIPS 201 have primacy; statements contained entirely within normatively referenced NIST publications are secondary; and statements entirely contained in FIPS 201 or normatively referenced NIST publications have primacy over normatively referenced standards of other origin."	Resolved by NIST-82.
NIST-2	NIST	Hildy	E				There is a sentence in Draft FIPS 201-2 as follows: The PIV Card shall be valid for no more than five years.	Correct the sentence to say: The PIV Card shall be valid for no more than six years.	Declined. The five year is in the track change version in the deleted section.
NIST-3	NIST	David Cooper	E				Some of the figures contain text that did not render correctly in the PDF.	Try to fix the text in Figures 3-1, 4-3, 4-4, 4-5, 4-6, 4-7, and 4-8.	Accept.
NIST-4	NIST	David Cooper	E				In many places where a reference appears at the end of a sentence, the reference is incorrectly placed after the period (e.g., "specified in SP 800-37. [SP 800-37]").	Move the reference to before the period (e.g., "specified in SP 800-37 [SP 800-37].").	Accept.
NIST-5	NIST	David Cooper	E	iv	117-121	3	The Explanation section contains information about implementation dates that are outdated: “As promptly as possible, but in no case later than eight months after the date of promulgation, executive departments and agencies are required to implement the standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities and logical access to controlled information systems.”	The outdated text should be removed or updated.	Resolved by GSA-1.
NIST-6	NIST	David Cooper	E	11	584	2.5.4	Neither the expiration date nor the FASC-N may be changed in a post-issuance update.	Change "The PIV Card expiration date or the FASC-N shall not be modified by a Post Issuance update." to "A Post Issuance update shall not modify either the expiration date or the FASC-N."	Resolved by replacing the sentence with “A post issuance update shall not modify the PIV Card expiration date, FASC-N, or UUID.”
NIST-7	NIST	David Cooper	E	16	754	3.1.1	This sentence is grammatically incorrect since the phrase "that are very similar to the card readers" does not restrict the set of card writers to which the sentence is referring.	Change sentence to "Card writers, which are very similar to the card readers, personalize and initialize the information stored on PIV Cards."	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-8	NIST	David Cooper	E	20		4.1.3	Section 4 should be reorganized since Section 4.1 is called "Physical Card Characteristics", but includes subsections on Logical Credentials and PIV Card Activation.	Limit Section 4.1 to physical card characteristics, and renumber Section 4.1.6 to Section 4.2 and renumber Section 4.1.7 to Section 4.3.	Resolved by AMAG-6.
NIST-9	NIST	David Cooper	E	21	896	4.1.3	The sentence is missing an article.	Change sentence to "Section 4.1.4.3 defines Zone 21F, where a raised surface may be placed."	Resolved by DoD-32.
NIST-10	NIST	David Cooper	E	23	943	4.1.4.1	Footnote 6 references the wrong section number.	Change Footnote 6 to "Alternatively, pseudonyms as provided under the law as discussed in Section 2.4.1."	Accept to change footnote to "Alternatively, an authorized pseudonym as provided under the law as discussed in Section 2.8.1."
NIST-11	NIST	David Cooper	E	23	958	4.1.4.1	The first sentence in this paragraph implies that 7 point font cannot be used.	Change paragraph to read "Departments and agencies shall use the largest font size of 7 to 10 points that allows the full name to be printed. The font size 7 point allows space for 3 lines and shall only be used if the full name is greater than 45 characters."	Accept.
NIST-12	NIST	David Cooper	E	23	962	4.1.4.1	The comma after "Employee" is misplaced.	Change sentence to read: An employee affiliation shall be printed on the card. Some examples of employee affiliation are "Employee," "Contractor," "Active Duty," and "Civilian."	Accept.
NIST-13	NIST	David Cooper	T	24	967-969	4.1.4.2	SP 800-73 states that the Agency Card Serial Number in the Printed Information buffer must be at most 10 bytes long and the SP 800-85B tool imposes a requirement that the Agency Card Serial Number in the Printed Information buffer be exactly 10 bytes long. However, Section 4.1.4.2 imposes no restrictions on the length of the Agency Card Serial Number.	The description of Zone 1B–Agency Card Serial Number in FIPS 201-2, the description of the Agency Card Serial Number in the Printed Information buffer in SP 800-73, and the requirements imposed on the Agency Card Serial Number by the SP 800-85B tool should be aligned.	Resolved by addressing the size of Agency Card Serial Number in SP 800-73. Increase the size of the Agency Card Serial Number in SP 800-73.
NIST-14	NIST	David Cooper	T	24	970-972	4.1.4.2	The description of the Issuer Identification Number is missing the five-digit number that follows the department and agency codes.	Change the description of Zone 2B–Issuer Identification Number to read "This item shall be printed as depicted in Figure 4-6 and consist of a six-character department code, a four-character agency code that uniquely identifies the department or agency (e.g., the four-character organizational code from [SP 800-87]), and a five-digit number that uniquely identifies the issuing facility within the department or agency."	Resolved by the revising text as follows: Zone 2B—Issuer Identification Number. This item shall be printed as depicted in Figure 4-6 and consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency.
NIST-15	NIST	David Cooper	E	38	1199	4.2.2	The issuer asymmetric signature is referred to as a file instead of a field.	Change sentence to "The issuer asymmetric signature field is implemented as a SignedData type, as specified in [RFC5652], and shall include the following information:"	Resolved by Cert-75. Correction will be done in SP 800-73.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-16	NIST	David Cooper	E	39	1219 – 1221	4.2.2	There has been some confusion about the requirements for the key used to sign the CHUID since the certificate corresponding to this key may assert the certificate policy id-fpki-common-devices, which permits the use of FIPS 140 Level 1 validated cryptographic modules. The text in this section and in Section 4.4.2 should make it clear that the key used to sign the CHUID and biometric data must be stored in a cryptographic module that has been validated to FIPS 140 with an overall Security Level 2 (or higher), which is the requirement stated in Appendix A.4 (or B.4 of FIPS 201-1).	Add a sentence to footnotes 10 and 14 that says "The cryptographic module used to generate the signature shall be validated to FIPS 140 with an overall Security Level 2 (or high) [FIPS140], as specified in Appendix A.4."	Declined. Section 4.2.2 and 4.4.2 (now Sections 4.2.1 and 4.2.3.2) no longer permit the assertion of id-fpki-common-devices in content signer certificates. Since all of the permissible policies that are now listed in these sections require the use of cryptographic modules that are validated to FIPS 140 level 2, the suggested sentence is no longer required.
NIST-17	NIST	David Cooper	E	25	1002	4.1.4.3	The commas and period should be placed inside the quotation marks.	Change sentence to read: Some examples of official roles are “Law Enforcement,” “Fire Fighter,” and “Emergency Response Team (ERT).”	Accept.
NIST-18	NIST	David Cooper	E	44	1391	4.4.1	This bulleted item ends with a period even though it is not the last item in the list.	The period at the end of this bulleted item should be deleted.	Resolved by new text.
NIST-19	NIST	David Cooper	T	44	1397 – 1412	4.4.1	Section 4.4.1 states that the right index finger shall be the primary finger unless it cannot be imaged. It then states that if only one fingerprint is used for authentication that the primary finger shall be used first. This will require most left-handed people to use their right index finger to authenticate, which will be very awkward for many left-handed people. It will also pose problems for people whose right index finger can be imaged but who have mobility problems with their right hand.	Changed Section 4.4.1 to state that when one fingerprint is used for authentication, either the primary or secondary finger may be used. If this is not an option, then applicants should be permitted to choose from which finger (e.g., left or right index finger) is the primary finger.	Accept to replace: The right and left index fingers shall normally be designated as the primary and secondary finger, respectively. However, if those fingers cannot be imaged, the primary and secondary designations shall be taken from the following fingers, in decreasing order of priority: 1. Right thumb 2. Left thumb 3. Right middle finger 4. Left middle finger 5. Right ring finger 6. Left ring finger 7. Right little finger 8. Left little finger with: The choice of which fingers to designate as primary and secondary is important and will vary between persons. The recommended selection and order appears in [SP 800-76]. (800-76 will repeat the ordering "index", "thumbs", "middle" "ring" then "little" but recommend user's own handedness guide which hand to use as primary).
NIST-20	NIST	David Cooper	T	44	1412 – 1414	4.4.1	This sentence states that authentication using the PIV Authentication key is the only alternative to authentication using fingerprints even though authentication using iris images is also a possibility.	Change sentence to read: "In cases where there is difficulty in collecting even a single live scan sample fingerprint of acceptable quality, the department or agency shall perform authentication using either iris images or asymmetric cryptography as described in Section 6.2.4.1."	Declined - this paragraph has been deleted.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-21	NIST	David Cooper	E	46	1456	4.4.2	Footnote 14 references the wrong section.	Change footnote to read "For legacy PKIs, as defined in Section 5.4, the certificates may be issued under a department or agency-specific policy that has been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level."	Accept.
NIST-22	NIST	David Cooper	T	47	1495 – 1501	4.5.4	Section 4.1.7.1 of Draft FIPS 201-2 specifically permits PIV Cards to be activated using verification data other than PINs. Requirements similar to those imposed on PIN input devices in Section 4.5.4 should be imposed on other verification input devices as well.	Generalize the text in Section 4.5.4 so that for physical access it requires any verification data input device (e.g., PIN pad, fingerprint reader) to be integrated with the reader. Similarly, for logical access require that if the verification data input device is not integrated with the reader then the verification data shall be transmitted securely and directly to the PIV Card for card activation.	Resolved by Cert-98.
NIST-23	NIST	David Cooper	E	61	1916	A.4	The reference to FIPS 140 is incorrect.	Change "[FIPS140-2]" to "[FIPS140]"	Resolved by ICAMSC-161.
NIST-24	NIST	David Cooper	E	49	1543	5.4	The title of this section is misleading since there is no requirement to migrate away from the use of legacy PKIs.	Change section title from "Migration from Legacy PKIs" to "Legacy PKIs"	Accept.
NIST-25	NIST	David Cooper	E	51	1588	6	The first sentence in Section 6 does not take into account that some of the authentication mechanisms described in Section 6 of FIPS 201-2 rely on features of PIV Cards that are optional.	Add a new sentence after the first one as follows: "This section defines a suite of identity authentication mechanisms that are supported by all the PIV Cards, and their applicability in meeting the requirements for a set of graduated levels of identity assurance. This section also defines some authentication mechanisms that make use of credential elements that may optionally be included on PIV Cards."	Accept.
NIST-26	NIST	David Cooper	E	53	1664	6.2.1	To be consistent with lines 1660 and 1161, the phrase "(back of card)" should be added to the end of line 1664.	Change line 1664 to "Zone 5B – Physical characteristics of cardholder (back of card)"	Accept. Also, insert space between dash and S on line 1665.
NIST-27	NIST	David Cooper	E	54	1709	6.2.3	The sentence is missing a preposition before "whom".	Change sentence to "As noted in Section 4.4, neither the fingerprint template nor the iris images are guaranteed to be present on a PIV Card, since it may not be possible to collect fingerprints from some cardholders and iris images are only required to be collected from cardholders from whom fingerprints could not be collected."	Resolved by GSA-27.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-28	NIST	David Cooper	T	55		6.2.3.1 and 6.2.3.2	The BIO and BIO-A authentication mechanisms should include a step to verify the signature on the CHUID. Also the final steps should allow for the use of identifiers other than the FASC-N.	Add a new second step to the BIO and BIO-A authentication mechisms that reads "The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered." Change the final steps for BIO and BIO-A to read "A unique identifier within the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access."	Resolved by requiring signature verification of the objects used to verify that the card is not expired. Resolved by NIST-81.
NIST-29	NIST	David Cooper	E	56	1765 – 1770	6.2.4.1	The last few steps in the description of PKI-AUTH are confusing since some of the steps are repeated. Also, it is unclear why the input to the access control decision needs to be the subject DN and a unique identifier.	Replace steps 6, 7, and 8 in Section 6.2.4.1 with: 6. The reader validates the PIV Authentication Key certificate from the PIV Card Application using standards-compliant PKI path validation to ensure that it is neither expired nor revoked and that it is from a trusted source. 7. The reader verifies that the response signature is the expected response to the issued challenge. 8. A unique identifier, such as the Subject Distinguished Name (DN) or the FASC-N, from the authentication certificate is extracted and passed as input to the access control decision.	Resolved by replacing steps 6, 7, and 8 in Section 6.2.4.1 (now Section 6.2.3.1) as follows: + The reader validates the PIV Authentication certificate from the PIV Card Application using standards-compliant PKI path validation to ensure that it is neither expired nor revoked and that it is from a trusted source. + The reader verifies that the card's response is the expected response to the issued challenge. + A unique identifier from the PIV Authentication certificate is extracted and passed as input to the access control decision.
NIST-30	NIST	David Cooper	E	57	1782 – 1785	6.2.4.2	Steps 4 and 5 in the description of PKI-CAK are confusing since some of the steps are repeated.	Replace steps 4 and 5 in Section 6.2.4.2 with: 4. The reader validates the Card Authentication Key certificate from the PIV Card Application using standards-compliant PKI path validation to ensure that it is neither expired nor revoked and that it is from a trusted source. 5. The reader verifies that the response signature is the expected response to the issued challenge.	Resolved by replacing steps 4 and 5 in Section 6.2.4.2 (now Section 6.2.3.2) with the following: + The reader validates the Card Authentication certificate from the PIV Card Application using standards-compliant PKI path validation to ensure that it is neither expired nor revoked and that it is from a trusted source. + The reader verifies that the card's response is the expected response to the issued challenge.
NIST-31	NIST	David Cooper	E	57	1796	6.2.5	The second sentence in Section 6.2.5 is missing a verb.	Change sentence to "A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC) authentication and the card responds with an indication of the success of the on-card biometric comparison."	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-32	NIST	David Cooper	E	57	1798	6.2.5	The fourth sentence in Section 6.2.5 is missing an article before the word "mechanism." There is also typographical errors in the following sentence.	Change sentences to "The PIV Card shall include a mechanism to block this authentication mechanism after a number of consecutive failed authentication attempts as stipulated by department or agency. As with authentication using the PIV biometric, if agencies choose to implement on-card biometric comparison it shall be implemented as defined in [SP 800-73] and [SP 800-76]."	Accept.
NIST-33	NIST	David Cooper	E	66	1997	E.1	The term “Approved” as defined in the Glossary is only used once within Draft FIPS 201-2, in the definition of “Hash Function”.	Delete the definition of “Approved”. In the definition of “Hash Function” change “Approved hash functions” to “Secure Hash Functions [FIPS180]”. Add a reference to FIPS 180 to Appendix F.	Accept.
NIST-34	NIST	David Cooper	E	66	2020	E.1	The term “Biometric System” does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of “Biometric System”.	Accept.
NIST-35	NIST	David Cooper	E	67	2035	E.1	The term “Claimant” is only used once within Draft FIPS 201-2, in the definition of PIN.	Delete the definition of “Claimant” and change the definition of PIN to “A secret that a cardholder...”.	Accept.
NIST-36	NIST	David Cooper	E	67	2040	E.1	The term “Conformance Testing” is only used once within Draft FIPS 201-1, in Appendix A.3.	Delete the definition of “Conformance Testing”.	Declined. Once mentioned is enough for it to be defined.
NIST-37	NIST	David Cooper	E	68	2053	E.1	The term “FASC-N Identifier” does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of “FASC-N Identifier”.	Accept.
NIST-38	NIST	David Cooper	E	68	2059	E.1	The term “Framework” as defined in the Glossary is only used twice in Draft FIPS 201-2, in the Acknowledgements Section and in the definition of the term “Architecture”.	Delete the definition of “Framework”.	Accept.
NIST-39	NIST	David Cooper	E	68	2064	E.1	The term “Graduated Security” does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of “Graduated Security”.	Accept.
NIST-40	NIST	David Cooper	E	68	2081	E.1	The term “Identity Binding” does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of “Identity Binding”.	Accept.
NIST-41	NIST	David Cooper	E	68	2084	E.1	The term “Identity Management System (IDMS)” does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of “Identity Management System (IDMS)”.	Accept.
NIST-42	NIST	David Cooper	E	70	2128	E.1	The term “PIV Issuer” is only used in the Glossary.	Delete the definition of “PIV Issuer” and eliminate its use in the definition of other terms.	Accept.
NIST-43	NIST	David Cooper	E	70	2133	E.1	The term “PIV Registrar” is only used in the Glossary.	Delete the definition of “PIV Registrar” and eliminate its use in the definition of other terms.	Accept.
NIST-44	NIST	David Cooper	E	70	2137	E.1	The term “PIV Sponsor” does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of “PIV Sponsor”.	Accept.
NIST-45	NIST	David Cooper	E	70	2139	E.1	The term “Population” does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of “Population”.	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-46	NIST	David Cooper	E	70	2156	E.1	The term "Reference Implementation" does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of "Reference Implementation".	Accept.
NIST-47	NIST	David Cooper	E	70	2160	E.1	The term "Secret Key" does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of "Secret Key" and add definitions for "Private Key" and "Symmetric Key".	Accept.
NIST-48	NIST	David Cooper	E	71	2165	E.1	The term "Trustworthiness" does not appear anywhere in Draft FIPS 201-2 other than in the Glossary.	Delete the definition of "Trustworthiness".	Accept.
NIST-49	NIST	David Cooper	E	71	2171	E.2	The following acronyms appear in Appendix E.2, but are not used in Draft FIPS 201-2:CFR, CVS, ECC, IDMS, RSA, SAVE, SF, USCIS	Delete the definitions of these acronyms from Appendix E.2.	Accept.
NIST-50	NIST	David Cooper	E	71	2171	E.2	The following acronyms are used in Draft FIPS 201-2, but do not appear in Appendix E.2: AID, IAW, ICAMSC, U.S.C., OCONUS, OCC, FSM, RMI, PII, SES, MWR, NCR, DOB, cm, mm, GSA, OGP, APL, CV, ASTM (Note: SES and MWR appear in Figure 4-5. NCR and DOB appear in Figure 4-8.)	Add definitions of the missing acronyms as follows: AID: Application IDentifier APL: Approved Products List ASTM: American Society for Testing and Materials cm: centimeter CV: Chain-of-trust Verification DOB: Date of Birth FSM: Federal States of Micronesia GSA: General Services Administration IAW: in accordance with ICAMSC: Identity, Credential, and Access Management Subcommittee NCR: National Capital Region mm: millimeter MWR: Morale, Welfare and Recreation OCC: On-Card Biometric Comparison OCONUS: Outside of Contiguous United States OGP: Office of Government-wide Policy PII: Personally Identifiable Information RMI: Republic of the Marshall Islands SES: Senior Executive Service U.S.C.: United States Code	Resolved by adding AID, ASTM, cm, DOB, GSA, ICAMSC, mm, MWR, OCC, PII, SES, and U.S.C. to the list of acronyms and by removing all uses of the acronyms APL, CV, FSM, IAW, OCONUS, OGP, and RMI.
NIST-51	NIST	David Cooper	E	71	2180	E.2	In the definition of CAK, "Card Authentication Key" is in bold.	Change "Card Authentication Key" to "Card Authentication Key".	Accept.
NIST-52	NIST	David Cooper	E			general	The words "section" and "appendix" should be capitalized whenever they precede a reference to a specific section number (e.g., Section 6.2.5)	Please review Draft FIPS 201-2 for correct use of capitalization.	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-53	NIST	Hildegard Ferraiolo	T	V	NA	8	The goal of NPIVP seems to be extended since FIPS 201-1. The previous FIPS 201 tasked NPIVP for the following:" The standard also covers security and interoperability requirements for PIV Cards. Funding permitting, NIST plans to develop a PIV Validation Program that will test implementations for conformance with this standard."	Replace: " NIST also developed a PIV Validation Program that tests implementations for conformance with this standard, and specifically with [SP 800-73]". with: " The standard also covers security and interoperability requirements for PIV Cards. For this purpose, NIST has established the PIV Validation Program that tests implementations for conformance with this standard as specified in SP 800-73 and SP 800-78.	Accept.
NIST-54	NIST	Hildegard Ferraiolo	T	13	310		SP 800-116 is missing in the enumeration of FIPS 201-related Special Publication	Add SP 800-116 to the enumerated list of special publication associated with FIPS 201-2	Declined, SP 800-116 provides recommendations, while the other Special Publications listed in 1.4 provide technical details for implementation.
NIST-55	NIST	Hildegard Ferraiolo	T	16	376	2.2	The Springer Memo seems to indicate that a NAC is sufficient to inially issue a PIV card, while FIPS 201-2 requires a at least a NCHC.	Resolve ambiguity or indicate which document (FIPS 201 or Springer Memo) is authoritive, in case of dis-alignment.	Resolved by OPM-2 and OPM-3.
NIST-56	NIST	Hildegard Ferraiolo	T	16	387	2.3	A FBI NCHC is required to issue a card, while the Springer Memorandum is satisfied with a NAC.	Resolve ambiguity or indicate which document (FIPS 201 or Springer Memo) is authoritive, in case of dis-alignment.	Resolved by OPM-2.
NIST-57	NIST	Hildegard Ferraiolo	T	17	411	2.3	The primary source documents cannot be expired or cancelled. How about the secondary identity source documents? Lines 428 though 434 indicate 'unexpired' source documents. Are all other 2ndary document allowed to be expired or cancelled?	Make an explicit statement for each of the 2ndary source documents to indicate if they can be expired or cancelled.	Resolved by NCE-8.
NIST-58	NIST	Hildegard Ferraiolo	T	19	480-484	2.4.1	The text in parenthesis is too long.	Suggest to remove parenthesis and make the text part of the paragraph, instead of parenthesis text. Another suggestion is to move the text in the parenthesis to a footnote.	Accept.
NIST-59	NIST	Hildegard Ferraiolo	T	19	491	2.4.2	An example of what grace period is, would be helpful.	Give an example of an employee in a grace period. Also: Make it explicit that Identity proofing and registration (section 2.3) is not required in order to issue a card for a person in grace period.	Resolved by Cert-20.
NIST-60	NIST	Hildegard Ferraiolo	T	19		2.5.1	Section 2.5.1 (Renewal) states that "The cardholder will not be allowed to start the renewal process if the original PIV Card is expired." It seems to be un-clear what process the issuer has to follow in this particular case.	Clarify what procedure (re-issuance?) should be followed in the case where a card has expired.	Resolved by DOT-15.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-61	NIST	Hildegard Ferraiolo	T	20	527	2.5.2	Section 2.5.2 states the reason for generating new asymmetric keys and certificate: in the re-newal process: New asymmetric keys are needed because the expiration of the certificates has to be before the Card's expiration date. This statement seems to be inaccurate. The reason to generate new keys for the new card is because the private key (in case of PKI-PIV and Dig. Sig key) has to be generated on-card and is not allowed to leave the card. Also make it explicit that a new FASC-N in the appropriate certificates are required.	In order to remove confusion, I suggest to remove the sentence that starts at line 527. Also replace: "Hence, a new PIV Authentication Key and certificate and a new asymmetric Card Authentication Key and certificate shall be generated." with "A new PIV Authentication Key, PIV Signature key and asymmetric Card Authentication Key shall be generated. The corresponding certificates (except for the Digital Signature key) will contain the new FASC-N, as per section 4.3."	Accept to delete sentence on Line 527. Insert "The expiration date of the certificate must be no later than the expiration date of the PIV Card." in Digital Signature Key description. Revise second sentence as: "A new PIV Authentication certificate and a new Card Authentication certificate shall be generated. The corresponding certificates shall be populated with the new FASC-N and UUID. For cardholders who are required to have a digital signature certificate, a new digital signature certificate shall also be generated. Key management key(s) and certificate(s) may be imported to the new PIV Card."
NIST-62	NIST	Hildegard Ferraiolo	E	21	604	2.5.5	typo	replace "their PIN" to "the PIN"	Resolved by USCPB-5.
NIST-63	NIST	Hildegard Ferraiolo	T	12	606	2.5.5	PIN reset as specified in SP 800-73-3 and ISO/IEC 7816-4 does not require CMS involvement. The reset command only needs to provide the new PIN followed by the PIN Unblock Key (PUK), which could be given to (and securely stored by) the cardholder. To enable local non-CMS PIN reset as requested at the business requirement meeting, local non-CMS PIN reset should be enabled. Additionally, OCC card activation should be a method as the 1:1 biometric match for the cardholder to receive a reset Card .	Replace the following two sentences: "PIN resets may be performed by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card.3" with "PIN reset may be performed locally through a dedicated, secure and un-networked device or remotely (e.g., post issuance update as per section 2.5.4). For PIV cards without On-Card biometric Comparison (OCC) card activation capability, the PIN reset procedure shall ensure that the cardholder's biometric matches the stored biometric through the BIO or BIO-A off-card authentication method before the reset PIV Card is provided back to the cardholder. For PIV cards with OCC card activation capability, the PIN reset procedure shall ensure that the cardholder's biometric matches the stored biometric through the OCC card activation method before the reset PIV Card is provided back to the cardholder. Departments and agencies may adopt more stringent procedures for PIN reset (including requiring in-person appearance or disallowing PIN reset, and requiring the termination of PIV Cards that have been locked); PIN reset procedures shall be formally documented by each department and agency.	Resolved by new remote PIN reset procedure.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-64	NIST	Hildegard Ferraiolo	T	22	612	2.5.5	Verification data reset (OCC card activation reset) does not require CMS involvement. To enable local non-CMS PIN reset as requested at the Business Requirement Meeting, Local non-CMS PIN reset should be enabled.	Replace the following two sentences: "Verification data other than the PIN may also be reset (i.e., re-enrollment) by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer shall either ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card or the biometric in the cardholder's chain-of-trust (see Section 4.4.1), or require the cardholder to provide a primary identity source document (see Section 2.3)." with "Verification data other than PIN may also be reset (i.e. re-enroll) either locally through a dedicated and secure device or remotely (e.g., post issuance update as per section 2.5.4). Before the reset PIV Card is provided back to the cardholder, the reset procedure shall either ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card or the biometric in the cardholder's chain-of-trust (see Section 4.4.1), or require the cardholder to provide a primary identity source document (see Section 2.3). PIN reset procedures shall be formally documented by the issuer."	Resolved by GSA-17.
NIST-65	NIST	Hildegard Ferraiolo	T	20	831	4	The biometric section 4.4 is not limited to mandatory biometrics.	Remove the word 'mandatory'	Resolved by deleting the referenced sentence.
NIST-66	NIST	Hildegard Ferraiolo	T	30	844	4.1	The contactless card side should also mention ISO/IEC 7816 as the application layer.	Replace "and ISO/IEC 14443 for contactless cards [ISO14443]." with ", ISO/IEC 14443 and ISO 7816 for contactless cards"	Declined. Section 4.5.2 (now Section 4.4.2) already addresses this.
NIST-67	NIST	Hildegard Ferraiolo	T	36	1028	4.1.4.3	19 F (optional) and 14 F (mandatory) both are reserved for expiration date, but use different formats. Should there be a statement that the date (Month and Year) should be the same in both field?	Make it explicit that 19F is the expiration date of the card. Currently it just states expiration date. State that the specified month and year of both field are the same, when the optional 19F field is populated.	Resolved by replacing label 'Expiration Date' with 'Card Expiration Date' in Figure 4-1 for Zones 19F and 14F. Also make 19F mandatory since it is the preferred placement of expiration date as indicated by comment resolution to SP 800-104. Label the font size of 14F as Arial 6 - 9pt Bold in Figure 4-1 as per OMB.
NIST-68	NIST	Hildegard Ferraiolo	T	35	1005	4.1.4.3	SP 800-104 has a precedence scheme associated with zone 15F. Should the precedence also be indicated in this section?	Suggested Text: Foreign National color-coding has precedence over Contractor color-coding. Foreign National, and Contractor color-coding have precedence over Emergency Response Official color-coding	Resolved by adding the following SP 800-104 precedence text in section 4.1.4.1: "Foreign National color-coding has precedence over Government Employee and Contractor color-coding. " (Note: resolution of Cert-60 removed "Red" and added "White")

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-69	NIST	Hildegard Ferraiolo	T	46	1125	4.1.6.1	Section 4.1.6.1 describes mandatory as well as optional data elements. It is important to describe the mandatory data element as the core credential set present on all PIV Card and thus support interoperable authentication mechanisms across agencies	Create a 'mandatory' logical credential subsection and optional credential subsection in section 4.1.6.1. In the mandatory logical credential subsection, describe the mandatory data element as the core credential set that are present in all PIV Card and thus support interoperable authentication across agencies. In the optional logical credential subsection, describe this subsection as follows: The PIV data model may be optionally extended to meet department or agency-specific requirements. If the data model is extended, this standard establishes requirements for the following logical credentials:	Resolved by revising the following sentence: "These mandatory data elements are part of the data model for PIV logical credentials, and include the following:" to "The following mandatory data elements are part of the data model for PIV logical credentials that support authentication mechanisms interoperable across agencies:"
NIST-70	NIST	Hildegard Ferraiolo	T	48	1190	4.2.1	Should it be explicitly mentioned that the expiration date of the CHUID shall match the expiration date printed on the surface of the card?	State that the expiration date of the CHUID shall match the expiration date printed on the surface of the card?	The text already states that both places specify the card expiration date.
NIST-71	NIST	Hildegard Ferraiolo	T	51	1284	4.3	add more clarity	Insert the word in bold: The PIV Card shall store a corresponding X.509 certificate to support validation of the asymmetric card authentication **public** key. Add 'public' to line 1303, 1311, 1287 as well.	Resolved by replacing "to support validation of the asymmetric card authentication key" with "to support validation of the public key" and by making similar changes on lines 1303 and 1311.
NIST-72	NIST	Hildegard Ferraiolo		52	1330 - 1337	4.4	With the introduction of on-card comparison (OCC) in addition to off-card comparison (BIO) the term accessible seems to be confusing with respect to contact/contactless access rights and with respect to PIN protection. Does it mean exportable for off-card comparison? Does it mean usable for on-card comparison? What type of data does the restriction apply to (life-scan or on-card biometric representation)?	Suggested re-wording: For off-card authentication (BIO, BIO-A, IRIS) purposes, the on-card biometric data shall be read exclusively over the contact interface and only after card activation. For on-card comparison (e.g., OCC, card activation), the on-card biometric data shall never be exported. The live-scan representation, however, may be transferred to the card through the contact or the contactless interface of the PIV Card to support card activation (section 4.1.7.1) and OCC authentication (section 6.2.x.x). In the case of OCC authentication, card activation is required prior to OCC authentication?. The biometric data shall be implemented and used in accordance with [SP 800-73] and [SP 800-76]. On-card biometric data shall not be used (export or import) for any other purpose other than BIO, BIO-A, OCC, card-activation, PIN rest and CMS (e.g., chain-of-trust) interactions.	Resolved by the following text in a new section titled "Biometric Data Access": The PIV biometric data, except for fingerprint templates for on-card comparison, that is stored on the card + shall be readable through the contact interface and after the presentation of a valid PIN; and + may optionally be readable through the virtual contact interface and after the presentation of a valid PIN. 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) and cardholder authentication (Section 6.2.2). The fingerprint templates for on-card comparison shall not be exportable. If implemented, on-card biometric comparison shall be implemented and used in accordance with [SP 800-73] and [SP 800-76].
NIST-73		Hildegard Ferraiolo	T	54	1414	4.4.1	The PKI-CAK is also an alternative authentication method when live scan biometric capture for BIO/BIO-A fails	Consider adding "and section 6.2.4.2" at the end of the sentence.	Resolved by indicating that PKI-AUTH is the recommended mechanism when live scan is not available.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-74		Hildegard Ferraiolo	T	54	1408	4.4.1	Suggest to clarify the 1:1 biometric match use-case.	Suggest to add the words in bold: "These fingerprint templates shall be used for 1:1 biometric verification **for physical and/or logical access** against live samples collected from the PIV cardholder (see Section 6.2.3).	Resolved by deletion of the paragraph.
NIST-75		Hildegard Ferraiolo	T	54	1400-1407 and 1411	4.4.1	Should the conditional-mandatory iris images, be specified in this section? What would be the order of 'preference or priority'? What would be the primary iris?	Specify order of priority for iris images, if needed. Also specify the primary image and order of use, as needed.	No change needed in FIPS 201. Instead FIPS 201 already cites [SP 800-76] for iris specifications. The SP will allow storage of either or both irises on the card and recommend storage of an image of the dominant eye if known. Agencies should be free to place only one iris on card - 800-76-2 allows this.
NIST-76	NIST	Hildegard Ferraiolo	T	54	1412 - 1414	4.4.1	Clarify the use of PKI-AUTH as an alternative to biometric authentication wrt 1) live-scan capture failure at authentication event vs. 2) no on-card fingerprint representation.	Suggest to clarify with a footnote that PKI-AUTH (or PKI-CAK) is the alternative authentication method when live-scan due to temporary injury at authentication event is not available. IRIS, on the other hand, is the alternative authentication method at access-points when biometric fingerprints are not available on-card due to permanent unavailability.	Resolved by GSA-27.
NIST-77	NIST	Hildegard Ferraiolo	T	58	1502	4.5.4	The requirements for the PIN input device is specified in this section. Shouldn't similar requirements be specified for live-scan readers for card activation (or OCC authentication) using OCC? A non-integrated live scan reader should also directly (and securely) transmit the live scan template to the PIV Card for card activation.	Add biometric live-scan reader requirements used for card activation via OCC.	Resolved by Cert-98.
NIST-78	NIST	Hildegard Ferraiolo	T	61	1888	6	The statement " This section defines a suite of identity authentication mechanisms that are supported by all the PIV Cards," is not completely correct. Because section 6 now also lists the authentication methods associated with optional credentials, not all cards will support the listed authentication methods.	Correct statement as follows: This section defines a suite of authentication method that are supported by the core (mandatory) credentials on all PIV cards. Section 6 also defines authentication methods that may be supported by optional credentials on some PIV cards.	Resolved by NIST-25.
NIST-79	NIST	Hildegard Ferraiolo	T	62	1647-1649	6	More emphasis should be applied to mandatory vs. optional credentials (wrt interagency interoperability) than what is mentioned in line 1647 - 1649. For clarity, the authentication mechanisms should be split up (sub-sectioned) with one section titled "Authentication mechanisms for Interoperable Interagency Use" and the other "Authentication Mechanisms supported by optional PIV card Credentials	Create two subsections: One section titled "Authentication mechanisms supported by the core mandatory credentials for Interagency Use" and the other "Authentication Mechanisms supported by optional PIV card Credentials. The first subsection should incorporate sections 6.2.1 through 6.2.4. Iris should be mentioned here as the mandatory alternative to fingerprint mach-off-card BIO/BIO(A). The second section should contain sections 6.2.5 through 6.2.6. Iris should be mentioned in this section as well as an additional optional authentication methods.	Resolved by deleting "Sections 6.2.1 through 6.2.4 define the basic types of authentication mechanisms that are supported by the core (mandatory) credential set on the PIV Card and are interoperable across agencies. Section 6.2.5 and section 6.2.6 define the authentication mechanisms that are available if the optional logical credential elements are present on the PIV Card."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-80	NIST	Hildegard Ferraiolo		66	1756-1757	6.2.4	The last sentence could in this paragraph could again add additional clarity wrt PKI-AUTH as alternative to BIO(A-).	Add a footnote to the last sentence of this section: PKI-AUTH is also the alternative authentication method in cases where live-scan biometrics could not be captured at the access point.	Resolved by deleting the third sentence of Section 6.2.4 (now Section 6.2.3). See GSA-27.
NIST-81	NIST	Hildegard Ferraiolo		62	1637	6.2	Some of the described authentication mechanisms specify the FASC-N to be used as identifier to be passed to the access control unit for access decision (BIO, BIO-A, PKI-CAK). Other authentication mechanisms just use a "unique identifier" (PKI-AUTH, CHUID, OCC).	Since Access Control (authorization) is out of scope of HSPD-12, I suggest to use 'unique identifier' to be passed to the access control unit in each authentication mechanism.	Accept. We will define a set of unique identifiers. The set will include the two mandatory identifiers, namely; FASC-N and UUID, which are present in all authentication credentials.
NIST-82	NIST CSD	Bill MacGregor	G	1		1.2	FIPS 201 is the "standard" required by HSPD-12. FIPS 201 references many other documents, however, to provide full detail of specification. It is possible (and has happened) that FIPS 201 and a referenced normative document may disagree. There is currently no explicit statement on resolution of such inconsistencies.	At the end of Section 1.2, add a *primacy clause* in a new paragraph: "This standard contains normative references to other documents, and to the extent decribed in each citation these documents are included by reference in this standard. Should normative text in this document [FIPS-201-2] conflict with normative text in a referenced document, the normative text in this document prevails."	Resolved by adding the following text to the first paragraph of Section 1.4: "This Standard contains normative references to other documents, and to the extent described in each citation these documents are included by reference in this Standard. Should normative text in this Standard conflict with normative text in a referenced document the normative text in this Standard prevails for this Standard."
NIST-83	NIST CSD	Bill MacGregor	E	45		4.4.2	The detail presented in this section is more appropriate to an SP than FIPS 201 itself.	Move the definition of the CBEFF_SIGNATURE_BLOCK to SP 800-76.	Accept per Cert-91/92.
NIST-84	NIST CSD	Bill MacGregor	E	2		1.3	The Change Management section may contain contain both general principles (guiding, but not normative) and specific requirements (normative). These are not separated at present.	Split the text of the Change Management section into Principles (informative), and Requirements (normative) sections.	Declined. Change Management section is not meant to add new requirements, but to ensure smooth transition and offer mitigation actions in regard to changes and new additions to the FIPS 201 specifications.
NIST-85	NIST CSD	Bill MacGregor	T	2		1.3	The Change Management section does not state many general operational principles--add the important ones.	Add and highlight operational principles such as: 1) to the extent possible, standards changes should not invalidate issued PIV Cards or require recertification of previously certified products; and 2) the number of in-person visits to the issuer should tend to an average of one to the sum of issuances, renewals, and reissuances per person.	Out of scope for the Change Management section.
NIST-86	NIST CSD	Bill MacGregor	T	41		4.3	Recent work on testing resistance to non-invasive attacks should be incorporated in FIPS 201-2. PIV Cards are unusually susceptible to non-invasive attacks because they are (millions of) cryptomodules that are small and constantly carried about; thus they are easily lost or stolen, presenting the acquirer with opportunities for extended and repeated probes.	Replace the sentence beginning "In addition to an overall validation of Level 2,..." with "In addition to an overall validation of Level 2, the PIV Card shall provide Level 3 physical security and Level 3 resistance to non-invasive attacks to protect the PIV private keys in storage."	Declined. While non-invasive attacks are addressed in the current draft of FIPS 140-3, they are not mentioned in FIPS 140-2, which is the version of the standard that is currently in effect. This issue will be revisited once FIPS 140-3 has been approved.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-87	NIST CSD	Bill MacGregor	T	42		4.3	Currently, one Key Management Key is designated as "active". However, this may be any one of "medium", "mediumHW", or "HIGH". This prevents the simultaneous use of medium and mediumHW, for example, that may be desirable to authorize multiple systems to received and decrypt email or other content. When both multi-platform and multi-level requirements are present, there may be no alternative other than multiple private keys and certs at different levels.	Consider allowing one, two, or three KMKs to be present at different levels, and "active". For example, this might be done by allowing one or two of what are now retired keys to become "active" keys at different levels.	Declined - The usability issues of several KMKs outweighs the benefits of the proposed change.
NIST-88	NIST CSD	Bill MacGregor	G	1		1.1	FIPS 201 contains policy, process, and technology requirements. The direct inclusion of technology requirements, in particular, makes it more difficult to adopt government or open standards to meet the policy requirements.	Consider refocusing FIPS 201 as an umbrella document connecting top-level policy (HSPD-12, OMB guidance, etc.) to profile documents; profile documents define process requirements and connect to other government and open standards through specification of profiles on their use. Although this might requirement substantial thought and reorganization, it would be a strategic improvement to better leverage open standards (in government) and government standards (in the private sector).	Resolved by moving some details to special publications and by keeping necessary 'shall' statements in the authoritative FIPS.
NIST-89	NIST CSD	Bill MacGregor	T	9		2.5	Is it sufficiently clear that an agency has discretion to require actions early? E.g., an agency should require biometric reenrollment whenever the biometric fails to verify, or the FRR becomes too high.	Add a statement to the effect that "Agencies may require PIV Card update, reissuance, or biometric enrolment more frequently than the maxium certificate, PIV Card, and biometric lifetimes stated here, to maintain the operational readiness of a cardholder's PIV Card. Shorter lifetimes may be specified by agency policy collectively, or on a case-by-case basis as sub-par operation is encountered."	Resolved by adding the follow text at the end of Section 2.5 (now Section 2.9): In order to maintain operational readiness of a cardholder's PIV Card, agencies may require PIV Card update, reissuance, or biometric enrolment more frequently than the maxium PIV Card and biometric lifetimes stated in this Standard. Shorter lifetimes may be specified by agency policy collectively, or on a case-by-case basis as sub-par operation is encountered.
NIST-90	NIST CSD	Bill MacGregor	T	55		6.2.3	BIO checks the CHUID for the expiration date of the PIV Card, but it does not check for revocation of the PIV Card.	Consider changing BIO to rely on the CAK or PKI auth cert instead of the CHUID. These should both be mandatory with FIPS 201-2, and both their expiration dates and PDVAL can be checked for card revocation. Or, if CAK is done before BIO, just eliminate the CHUID read requirement.	Resolved by allowing use of other data elements (see Cert-101). Resolved by adding "Does not provide protection against use of a revoked card." bullet under characteristics. Note that the signature verification may require retrieval of content signer certificate from the CHUID if the signature on the biometric was generated with the same key as the signature on the CHUID.
NIST-91	NIST CSD	Bill MacGregor	T	55		6.2.2	CHUID is inherently weak as an authenticator, since it does not rely on a secret that can be reliably preserved. In the time since FIPS 201 was published, and with the change of CAK to mandatory issuance, use of CHUID should be officially discouraged.	Insert text stating that the CHUID is deprecated and is expected to be removed from FIPS 201 at the next five year revision.	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-92	NIST CSD	Bill MacGregor	E	37		4.1.6 through 4.4.2	These sections on Logical Credentials lack a clear, high-level introduction.	Consider adding a short introduction that describes the base and optional functions of a PIV-conformant electronic module, in such a way that it could be implemented in any suitable physical cryptomodule. One benefit: at the module level, it should be possible to specify one FIPS 140-2 security policy for all PIV implementations e.g., in SP 800-73.	Resolved by AMAG-6. Also: Cryptographic module requirements remain unchanged and are specified close to Section 4.1.6 (now Section 4.2). Derived credentials will be addressed in a new Special Publication.
NIST-93	NIST CSD	Bill MacGregor	T	2		1.3	Introduce terminology "migration" and "adoption".	Migration is a general or complete transition to a non-backward-compatible feature Adoption is a selective transition to use an optional feature. The normative part of Change Management should list the non-backward-compatible and optional features added to FIPS 201-2, and list migration and adoption plans that should be developed.	Noted. Resolved by ES-2. Resolved by DOJ-1.
NIST-94	NIST CSD	Bill MacGregor	E	49		5.5	The language in the second paragraph is illogical.	Replace the third sentence with "However, an authentication certificate (and its associated key pair) may be revoked and then immediately replaced with a new certificate (and its new associated key pair) without revoking the PIV Card." Also, explain the case that is not discussed: "If one or both authentication certificates has expired, but the expired certificate(s) are not reported as revoked and the PIV Card has not yet expired, applications that perform PDVAL should consider the card suspended until the key generation(s) and certificate update(s) are done."	Declined. Adding the word 'immediately' would change the requirements in a way that is not warranted.
NIST-95	NIST CSD	Bill MacGregor	G	38		4.1.6	The Printed Information Buffer is not described in FIPS 201. In discussions on visual name field, agencies have stressed the importance of access to (a) full legal name in the PIB.	Call out a requirement for the PIB in the bulleted list on page 38. The PIB should contain all of the variable printed (text) information on the PIV Card. Because the PIB is relatively small, make it mandatory. Prohibit abbreviation of name components in the name field in the PIB.	Declined and out of scope -- FIPS 201 lists authentication related data elements - other non-authentication data elements such as the Card Capability Container, the Security Object, and the Printed Information Buffer may be specified and addressed in SP 800-73.
NIST-96	NIST CSD	Bill MacGregor	T	9		2.4.1	As written in the draft, the Special Rule for Pseudonyms appears to leave the decision to use pseudonyms up to the agencies -- "an agency has formally authorized the use of a pseudonym" is all it says. This means the policy is up to the agencies, and the result could be a different policy in each agency. According to Section 4.1.4.1, a pseudonym substitutes for the full name--so recognition might not be possible. Use of pseudonyms should be further limited.	Change "In cases where an agency has formally authorized the use of a pseudonym," to "When an agency decides that use of a pseudonym is necessary to protect an employee or contractor from physical harm or severe distress due to the possible actions of another person, the agency may authorize a pseudonym for use by the employee or contractor. The card issuer shall issue..."	Resolved by new text.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
NIST-97	NIST	Bill MacGregor	T				Through an exchange with SP 800-63-1 authors last week, I discovered that old issues regarding the relationship of FIPS 201 to SP 800-63/-63-1 were partially, but not completely, resolved. There may be residual issues that should be examined in Draft FIPS 201-2 comment resolution. Assumption: All valid PIV Cards should be SP 800-63/-63-1 Level 4 credentials. If this assumption is correct, then all identity proofing actions, in particular, should meet SP 800-63/-63-1 requirements (and, CPF requirements). Looking at those documents some time ago, there are these constraints at Level 4:1) The primary document must be a government ID; the secondary document must be an "independent" government ID or a financial account. Since FIPS 201 does not recognize financial accounts, the intersection is that both documents must be government IDs. 2) Both government IDs must be valid. 3) Both government IDs must be photo IDs. Because several of the requirements on the I-9 secondary list are not photo IDs, SP 800-63-1 authors agreed to drop the photo ID requirement on the secondary government ID in SP 800-63-1. (Note that the photo ID requirement on the secondary document is present in SP 800-63.)	Suggested Draft FIPS 201-2 changes: 1) Check the FIPS 201-2 secondary ID list for non-government IDs, and remove any that are found. A quick scan turned up only "student ID" as a possible non-government ID. 2) Require that all FIPS 201-2 IDs listed are, on physical examination, not apparently expired or cancelled. (Documents without an expiration date should be presumed valid indefinitely.) 3) Check that the identity proofing section is also consistent with CPF requirements.	Resolved by: 1) Agree to remove 'student ID' on the basis that it can be easily forged. 2) Accept. 3) Noted.
NIST-98	NIST	Hildy	T	52	1653	6.2	Sections 6.2.1 through 6.2.4 define the basic types of authentication mechanisms that are supported by the core (mandatory) credential set on the PIV Card and are interoperable across agencies. Section 6.2.5 and section 6.2.6 define the authentication mechanisms that are available if the optional logical credential elements are present on the PIV Card.	Suggest removing the iris from section 6.2.1. It is currently part of BIO and BIO-A, which are tagged as the mandatory credential for interoperable cross-agency use. Instead, we need to define a iris authentication method in the optional authentication methods.	Resolved by NIST-79 and GSA-27.
NNSA-1	NNSA Y-12 Site Office	Sharon Daly	G			G	Request a clarification regarding Section 2.4. regarding, "... synchronize lifecycles of card, certificates, and biometric data." Does this mean that since the PIV Card maximum life increases from 5 to 6 the certificates and biometric data also increases to 6? If not, there really isn't a change based on the fact that the certificate lifecycle is significantly less than the badge. In that case, the use and implication of "synchronize" appears to be inaccurate or misleading since the certificate lifecycle would definitely not "match" the badge life. Could this be clarified to include, if different, the certificate lifecycles in writing and in the FIPS 201-2.		FIPS 201-2 states that biometric data may be used for at most 12 years, which is twice the maximum validity period of a PIV Card. The Common Policy currently specifies a maximum certificate validity period of 3 years, which is half the maximum validity period of a PIV Card. In this way, the maximum validity periods are synchronized (even multiples of each other) even though they do not match. Decline to specify maximum certificate validity periods in FIPS 201-2, as this would preclude the Federal PKI Policy Authority from making changes to this in the Common Policy.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OPM-1	OPM FIS Operational Policy	Tammy Paul 703-305-1006	G	4	331-332	1.4	Executive Order 13467 assigns the Office of Personnel Management as Suitability Executive Agent, responsibility of developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to suitability and eligibility for logical and physical access. The phrasing of this sentence implies that the information provided in Appendix B could be sufficient to address the requirement. Suggest rephrasing to emphasize that the authority governing the background investigations process is not in FIPS, but rather elsewhere.	Appendix B, Background Check Descriptions, provides information on background investigations. This appendix is informative.	Resolved by deleting Appendix B per OPM-6.
OPM-2	OPM FIS Operational Policy	Tammy Paul	G	6	386-389	2.3	The NACI is the minimum investigation required for issuing a PIV. Non-federally conducted investigations do not meet the HSPD-12 requirement. The term "or equivalent" implies that a non-federal investigation could meet the requirement, especially if considered with Appendix B as written. Suggest rephrasing to emphasize that the investigation level has to be equivalent to, at minimum, a NACI, and it has to be conducted to and in accordance with federal investigative standards. In addition, this terminology may be problematic since the "NACI" equivalent probably will be called "Tier 1."	The Process shall begin with initiation of a NACI investigation. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI or higher federal background investigation.	Resolved by replacing: "The process shall begin with initiation of a NACI or equivalent. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI." with: + The process shall begin by locating and referencing a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation record. In the absence of a record, the process shall ensure 1) the initiation of a Tier 1 or higher federal background investigation and 2) the completion of the Automated Record Checks (ARC) of the background investigation. In cases where the ARC results are not received within 5 days of the ARC initiation, the FBI NCHC (fingerprint check) portion of the ARC shall be complete before credential issuance." Also note that further requirements are specified in OPM and OMB policies and HSPD-12 FAQs guidance.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OPM-3	OPM FIS Operational Policy	Tammy Paul	G	8	457-458		This is the same problem as above with using the terminology of "NACI or equivalent." Suggest rephrasing.	The process shall ensure the initiation of a NACI investigation. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI or higher federal background investigation.	Resolved by replacing bullet # 3 with: "+ Before issuing the identity credential, the process shall ensure that a previously completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation is on record. In the absence of a record, the required federal background investigation shall be initiated. The credential should not issued before the results of the ARC are complete. However, if the results of the ARC have not been received in 5 days, the identity credential may be issued based on the FBI NCHC. In the absence of an FBI NCHC (e.g. due to unclassifiable fingerprints) the ARC results are required prior to issuing a PIV credential. The PIV Card shall be revoked if the results of the background investigation so justify." Note: - requirements are also included in OPM and OMB policies and through HSPD-12 FAQs guidance.
OPM-4	OPM FIS Operational Policy	Tammy Paul	E	10	563	2.5.2	"NACI check" sounds awkward. Suggest rephrase.	"NACI background investigation"	Resolved by Replacing: "If the expiration date of the reissued PIV Card is later than the expiration date of the old card, the card issuer shall ensure a proper authority has authorized reissuance of the credential and the NACI check is followed in accordance with OPM guidance." with: "If the expiration date of the reissued PIV Card is later than the expiration date of the old card, the card issuer shall ensure that a proper authority has authorized reissuance of the credential, and that a re-investigation is performed if required, in accordance with OPM guidance."
OPM-5	OPM FIS Operational Policy	Tammy Paul	E	11	568	2.5.2.1	"People's names" sounds awkward. Delete "people's"	Names often change as a result….	Resolved by DoD-23.
OPM-6	OPM FIS Operational Policy	Tammy Paul	G	62	1935	Appendix B	The inclusion of a description of a NACI may lead one to the erroneous conclusion that FIPS-201 establishes the federal investigative standards. Suggest deleting Appendix B. Alternatively, include a paragraph that refers questions about background investigations to a federal personnel security entity or to OPM, as the Suitability Executive Agent under E.O. 13467.	either delete or add new paragraph	Accept to delete Appendix B. In addition: Include a link to OPM's Tiered investigative standard in the References section and by footnote in Section 2.2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
OPM-7	OPM FIS Operational Policy	Tammy Paul	E	63	1949	Appendix C	"intend" should be "intended"	add "ed'	Resolved by deleting Appendix C.
OPM-8	OPM FIS Operational Policy	Tammy Paul	G	66	1991-1992	Appendix E	an Applicant could also be an "affiliate" if the person needs an investigation per OMB Memo 05-24	include "government affiliate" in list	Resolved by including government affiliate and adding a footnote to point to M-05-24 page 2 for further detail of an affiliate.
OPM-9	OPM FIS Operational Policy	Tammy Paul	E	70	2164	Appendix E	Usually the term being defined is not included in its definition.	delete "to comply with the standard."	Resolved by removing definition.
OPM-10	OPM FIS Operational Policy	Tammy Paul	G	71	2193		CVS stands for "Central Verification System"	Replace "Clearance" with "Central"	Resolved by NIST-49.
PB-1	Precise Biometrics	Michael Harris	E	2	274	1.3.3	The document states "The preferred (and standardized) replacement for the trademarked term "match on card" is on-card comparison". Precise Biometrics holds trademark to "Precise match on card" however, the more generalized and accepted terminology as 'match on card' is not trademarked and freely open for use. Most importantly, the term "match on card" is more generally accepted, in use and recognizable in the biometric industry.	Continue use of terms "match on card" and "MOC" when used in existing and new industry specifications. Precise Biometrics holds trademark to "Precise Match-on-Card" and other similar IP/marks that generally or more directly describe technology and functions related to our core business or IP. Precise Biometrics contends that over the years, "match-on-card" has become synonymous within the industry as the process for performing biometric comparison, i.e., matching, within the secure confines of the ICC component within the smartcard. Precise Biometrics thereby recommends the continued use of match-on-card and shall freely allow use of this common language to describe the aforementioned processes. No claims or actions will be pursued by Precise Biometrics against such use nor does Precise Biometrics forsee any conflicts of interest or value to the use of "match on card" in relation to our trademark "Precise Match-on-Card" It is unnecessary to introduce a new and potentially confusing term such as 'on card comparison'	Solved by IBIA-1.
PB-2	Precise Biometrics	Michael Harris	G	na	na	all	For consistency, SP 800-73 part 1 should be updated in Appendix B and section 3 to allow for fingerprint data to use local processing. SP 800-73 part 2 should be updated to define cases where MOC can be used as the alternative to global PIN, PIV PIN, or both.	Update 800-73 to treat data in a larger context than stored on card. The PIN Alternate use cases should be defined.	Noted. This comment is made against SP 800-73 and as such is out of scope. Our intention is to modify all Special Publications related to PIV to account for such changes.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
PB-3	Precise Biometrics	Michael Harris	G	na	na	all	The relationship between the mandatory fingerprint data for external verification and FBI background check, and the optional MOC fingerprint template data should be defined: one or more enrollments, chain of trust, etc.	Propose adding to chapter 2 to further clarify and distinguish between fingerprint data types.	Accept as follows: Text in the existing FIPS 201-2 draft, in section 4.4.1 (now Sections 2.3 – 2.6), explains this. So acceptance of AMAG-6 will result in the existing text being relocated to section 2.
PB-4	Precise Biometrics	Michael Harris	G	na	na	all	Note that by design the MOC templates may not be read out from the card, thus are unavailable for reissuance or renewal data as new card input.	Propose clarification in Sections 2.5.1 and 2.5.2	Accept as follows: Text in the existing FIPS 201-2 draft, in section 4.4.1 (now Sections 2.3 – 2.6), explains this. So acceptance of AMAG-6 will result in the existing text being relocated to section 2.
PB-5	Precise Biometrics	Michael Harris	G	12	603	2.5.5	This section should be updated if MOC is to be used as a means for PIN reset.	Detailing MOC as an alternate for PIN reset would offer great advantage to PIV and card administration	Resolved by new remote PIN reset procedure.
PB-6	Precise Biometrics	Michael Harris	E	16	744	3.1.1	Section should be updated to reflect the use of MOC offering the same functionality as PIN.	Update section to confirm that MOC offers PIN functionality.	Resolved by amended text and the following footnote: Alternatively, on-card biometric comparison can be used to activate the PIV card.
PB-7	Precise Biometrics	Michael Harris	T	37	1142	4.1.6.1	We assume that on-card biometric "comparison data" refers to the templates.	Suggest using the term match on card templates as this is the more common use and description	See DoD-50.
PB-8	Precise Biometrics	Michael Harris	T	37	1161	4.1.7.1	Line states that "Other card activation mechanisms, only as specified in [SP 800-73], may be implemented and shall be discoverable."	Future versions of Sp 800-73 must included MOC as PIN alternate for consistency	See PB-2.
PB-9	Precise Biometrics	Michael Harris	T	42	1330-1337	4.4	It is incorrect to state that the on-card comparison data (moc template) may be read out from the card. It is only the MOC function that is made available through the card edge interface	Rephrase this paragraph for accuracy	See NIST-72.
PB-10	Precise Biometrics	Michael Harris	E	44	1416-1458	4.4.2	There is no explicit definition for the MOC biometric templates	Suggest explicitly defining biometric templates or expressly excluding this data from the definition	Replace: The integrity of the mandatory fingerprint and optional iris and facial data records shall be protected using digital signatures as follows. With: "The integrity of all biometric data, except for fingerprint templates for on-card comparison, shall be protected using digital signatures as follows."
PB-11	Precise Biometrics	Michael Harris	T	47	1496-1501	4.5.4	Should logically be extended to cover fingerprint input devices when used with MOC. As MOC is presented as an alternate to the PIN this should be a referenced device implementation.	Suggest explicitly defining the use of MOC as a PIN alternate	Resolved by Cert-98.
PB-12	Precise Biometrics	Michael Harris	T	54	1702	6.2.3 - 6.2.3.2	Should logically be extended to define MOC as an alternative to the PIN.	Suggest explicitly defining the use of MOC as a PIN alternate	Declined. There is a security and privacy risk in using OCC to read stored biometric data from the card. Cardholder activation via PIN entry is required to read the biometric.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
PB-13	Precise Biometrics	Michael Harris	T	56	1760-1761	6.2.4	Should logically be extended to define MOC as an alternative to the PIN.	Suggest explicitly defining the use of MOC as a PIN alternate	Resolved by the following changes: - Combine steps 2 and 3. - Add a sentence – If implemented, other card activation mechanisms, as specified in [SP 800-73], may be used to activate the card. - Change the characteristics to - Strong resistance to use of unaltered card by non-owner since card activation is required.
SCA-1	SCA PAC & IC	Gilles Lisimaque, IDTP	G	iv	169	9	"This standard is effective immediately." The standard cannot be implemented until other documents are updated (e.g., SP 800-73, FIPS 140-3, SP 800-96, GSA APL and test specifications, SP 800-116, SP 800-78). A timeline for updates to all documents is required.	Revise to: Implement as quickly as possible with timeline and new special publications that reflect changes to supporting documents.	Resolved by DoD-3.
SCA-2	SCA PAC & IC	Gilles Lisimaque, IDTP	G	iv	169	9	"This standard is effective immediately" may not be easy to put into practice. It changes some of the existing practices and has impact on other standards (e.g., SP800 series), as well as qualification processes not yet defined. It would be more accurate to indicate that this standard replaces and supersedes the previous version.	Suggested sentence: "This standard replaces the previous version and will take effect as soon as all related technical standards have been updated." OMB should provide an effective date.	Resolved by DoD-3.
SCA-3	SCA PAC & IC	Gilles Lisimaque, IDTP	G	2	251	1.3	The sentence indicates that this standard may impact existing implementations. This is the case, for example, for agencies which did not previously implement an asymmetric CAK. Will there be a timetable for migration and indications on how to cope with the transition?	Indicate in a note, or by adding a sentence, that a "migration document" will be issued allowing the impact of such changes to be minimized.	Resolved by DOJ-1.
SCA-4	SCA PAC & IC	Gilles Lisimaque, IDTP	G	2	270	1.3.2	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. See separate document, 'PIV Card AiD Issue-Solution - 051311.docx' for one possible approach for application version discovery.	Add: Such changes may affect FISMA, C&A and FIPS 140 certifications as well as, over time, result in an increasingly complex card discovery process at the relying subsystems. Also: See separate document, 'PIV Card AiD Issue-Solution - 051311.docx' for one possible approach for application version discovery.	Declined to include proposed text.
SCA-5	SCA PAC & IC	Bob Dulude, ActivIdentity	E	2	274	1.3.3	Document defines and uses a new acronym OCC while industry uses the more common phrase "match on card" or MOC. In other places in the document the phrase "cardholder-to-card" or CTC is used (e.g., line 1795) is used.	Establish consistency within the document.	Resolved by IBIA-1
SCA-6	SCA PAC & IC	Lars Suneborn, HIRSCH	G	3	276	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. 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 the current systems. The systems will need to be updated if an agency decides to support the OCC authentication mechanism.	Add: System changes may affect current FISMA and C&A status.	Declined to include proposed text.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-7	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	3	287	1.3.5	Components that may be affected by version management include, for example, PIV cards, PIV middleware software, and card issuance systems. The current language does not include relying systems and possible consequences of change.	Change sentence to: Components that may be affected by version management include, for example, PIV cards, PIV middleware software, card issuance and relying systems Such system changes may affect current FISMA and C&A status on applicable system components.	Declined to include proposed text. The list of components is not all inclusive.
SCA-8	SCA PAC & IC	Gilles Lisimaqu e, IDTP	E	5	374	2.1	"An issued credential is not modified, duplicated, or forged." Credentials can be updated by the issuers (e.g., update of the PKI-AUTH certificate when a new key is generated in the card). Suggested to add the word "illegitimate" to the sentence.	Suggested modified sentence: "An issued credential is not modified, duplicated or forged by an illegitimate party."	Resolved by revising the sentence to "An issued credential is not duplicated or forged, and is not modified by an unauthorized entity."
SCA-9	SCA PAC & IC	Jason Rosen, NASA	G	8	386	2.3	FIPS 201-2 should consider a National Security Background investigation conducted at the Secret Level or higher as equivalent to the NACI for identity proofing, at the agency's discretion.	A National Security Background investigation conducted at the Secret Level or higher that is within its valid time period should suffice to issue a PIV or PIV-I card.	Noted. National Security Background Investigation is covered by M-05-24 3b and 3d. In addition, FIPS 201 mentions 'equivalent or higher' investigation, which includes the NACLC. See also http://www.idmanagement.gov/pages.cfm/page/IDManagement-HSPD12-frequently-asked-questions Question 1: Can a National Agency Check with Law and Credit (NACLC) be used for PIV credential issuance? Answer: The NACLC is often used as the minimum investigative requirement for access to Secret information and below for military service personnel and Federal contractors. For purposes of PIV credential issuance, the NACLC satisfies the essential requirements.
SCA-10	SCA PAC & IC	Gilles Lisimaqu e, IDTP	E	6	410	2.3	Is the Department of Defense Common Access Card referenced here the transitional card, or the DoD CAC with a PIV applet onboard, or any of them? Does this mean any CAC?	Replace the sentence with: "A legacy Department of Defense Common Access Card" or clarify what type of CAC is acceptable.	Resolved by replacing the Common Access Card with the PIV Card on the list.
SCA-11	SCA PAC & IC	Walter Hamilton , IBIA	G	8	468	2.4	The minimum accuracy requirements for biometric matching using iris recognition technology is not yet specified in SP 800-76.	It is assumed that OMB will issue guidance that indicates that the requirement for iris recognition, as an alternative to fingerprint matching, will be effective following an update to SP 800-76.	Iris imaging is now optional, per DOT-11.
SCA-12	SCA PAC & IC	Jason Rosen, NASA	G	8	472	2.4	FIPS 201-2 states: "The PIV Card shall be valid for no more than six years." Renewing or re-issuing certificates to an existing PIV card during its life is complex. It is recommended that FIPS 201 allow the certificate expiration be synchronized with the card expiration, up to a limit of six years.	The card and the certificates should be able to synchronize expiration. Certificates should be able to be synchronized with card life, to ease renewal or re-issuance of certificates.	Out of scope: Maximum certificate lifetime is specified in COMMON, which is under the control of the Federal PKI Policy Authority. The lifecycle can be synchronized with certificates by issuing cards with a 3 year validity period.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-13	SCA PAC & IC	Walter Hamilton, IBIA	E	9	484	2.4.1	An open parenthesis is missing in the sentence.	Add an open parenthesis before the word "which."	Resolved by NIST-58.
SCA-14	SCA PAC & IC	LaChelle LeVan, Probaris	G	9	493	2.4.2	The Grace Period specifies "In instances where such an interregnum does not exceed 60 days, a card issuer shall issue the employee or contractor a new PIV Card in a manner consistent with PIV Card Issuance." This requirement may be interpreted as two different scenarios and a clarification is suggested: Scenario 1: Employee or contractor starts a PIV Issuance process for a new credential (the first credential from the affiliated agency). During the initial process for PIV Card Issuance, a lapse of time occurs - not to exceed 60 days - where the employee or contractor may temporarily have a lapse of affiliation. If this lapse does not exceed 60 days, the employee or contractor may resume the original PIV Card Issuance process to receive a credential. Scenario 2: Employee or contractor has a current PIV credential, and their affiliation with the agency lapses. The original PIV credential is revoked. In a period of time - not to exceed 60 days - the employee or contractor is once again affiliated with the agency. In this scenario, if the 60 day time limit has not been exceeded, a card issuer shall issue a new PIV credential in a manner consistent with PIV Card Reissuance.	Proposed Change (scenario 1): In some instances an individual's status as a Federal employee or contractor will lapse for a brief time period during the PIV Card Issuance process. In instances where such an interregnum does not exceed 60 days, a card issuer shall continue to issue the employee or contractor a new PIV Card in a manner consistent with PIV Card Issuance. Proposed Change (scenario 2): In some instances an individual's status as a Federal employee or contractor will lapse for a brief time period. In instances where such an interregnum does not exceed 60 days, a card issuer shall reissue the employee or contractor a new PIV Card in a manner consistent with PIV Card Reissuance.	Resolved by Cert-20.
SCA-15	SCA PAC & IC	Jason Rosen, NASA	G	10	506	2.5.1	FIPS 201-2 should consider a National Security Background investigation conducted at the Secret Level or higher as equivalent to the NACI for identity proofing, at the agency's discretion.	A National Security Background investigation conducted at the Secret Level or higher that is within its valid time period should suffice to issue a PIV or PIV-I card.	Resolved by SCA-9.
SCA-16	SCA PAC & IC	Walter Hamilton, IBIA	G	9	514	2.5.1	The minimum accuracy requirements for biometric matching using iris recognition technology will be specified in SP 800-76-2. FIPS 201-2 needs a supporting reference for minimum accuracy for biometric matching using iris recognition technology.	Update FIPS 201-2 to reference SP 800-76-2.	See IBIA-3.
SCA-17	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	10	525	2.5.1	Renewal of card: The digital signature must be recomputed with the new FASC-N. A new FASC-N may require re-registration in relying systems.	Add: The re-issued card will have a new Credential Number,CN. This results in a new FASC-N. The digital signature must be recomputed with the new FASC-N and the new credential must be re-registered/re-enrolled into the relying system	Out of scope. Not all relying systems may use FASC-N as basis for access. Access control is out of scope.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-18	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	10	553	2.5.2	Add SCVP path validation	Change to: Online Certificate Status Protocol (OCSP) and Server-based Certificate Validation Protocol (SCVP) devices shall be updated so that queries with respect to certificates on and the issuer of a PIV Card can be answered appropriately.	Declined. An OCSP responder may either be operated on behalf of the relying party (a locally-trusted OCSP responder) or by (or on behalf of) the CA. In FIPS 201-2, references to OCSP are only for OCSP responders operated by (or on behalf of) the CA. An SCVP server can only be operated on behalf of the relying party. While we do not discourage the deployment and use of SCVP, it is out-of-scope for FIPS 201-2.
SCA-19	SCA PAC & IC	Sal D'Agosti no, IDmachi nes	G	10	553	2.5.2	Current references to OCSP, SCVP and CRL are in Appendix F. Does NIST consider following the standards as normative?	Add references to OCSP, SCVP and CRL standards as normative.	SCVP is not mentioned in FIPS 201 and therefore, does not need to be included in Appendix F (now Appendix D). The references in Appendix F (now Appendix D) are provided for informative purposes only. However, the main body of FIPS 201 will establish whether these reference (or part of) are normative.
SCA-20	SCA PAC & IC	Jason Rosen, NASA	G	10	557	2.5.2	Eighteen hours for revocation notification is too long in exigent circumstances in which a person's life or safety is at risk.	We recommend that NIST investigate and provide further guidance on mechanisms and policy for faster notification across agencies of credential revocation requests for exigent circumstances in which a person's life or safety is at risk.	Declined. Procedures for de-authorizing the use of PIV Cards faster than certificate revocation information can be distributed is best left to agency discretion.
SCA-21	SCA PAC & IC	Gilles Lisimaqu e, IDTP	T	11	583	2.5.4	This paragraph should mention that the Security Data Object may also have to be updated as a consequence of other updates.	Suggested adding a sentence saying: "The Security Data Object in the card shall be updated to reflect any changes made by such modifications."	Resolved by NIST-95.
SCA-22	SCA PAC & IC	Gilles Lisimaqu e, IDTP	E	12	607	2.5.5	Verifying that the cardholder biometric stored on the card matches the user may be difficult when the user has forgotten the PIN. This appears to assume that the verification is performed by comparing biometric data stored outside of the card or that there is issuer direct access to the biometric data in the card. Recommended best practice should be described.	Describe the procedure to reset the PIN and verify its biometric information from the card when the PIN has been forgotten by the cardholder.	The text stated: "Before the reset PIV Card is provided back to the cardholder, the card issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card" Note that the card may be reset before the biometric comparison is performed. More detailed description of the PIN reset procedure has been added.
SCA-23	SCA PAC & IC	LaChelle LeVan, Probaris	G	12	615	2.5.5	The inclusion of the option to allow the cardholder to provide a primary identity source document to receive the credential after a PIV Card Verification Data Reset (e.g., PIN reset) undermines the security and intent of the other processes. The cardholder does not have a "something you know" factor (unknown PIN); the cardholder does not have a "something you have" factor (token has been updated by issuer and the cardholder needs to validate his/her identity to get the card back); the cardholder only has a "something you are" factor which is the biometric. This biometric can be compared to the token (PIV card) or the issuing system. The inclusion of an option for presenting an identity source document, which as written currently may or may not be able to "reconnect the chain of trust" to the original PIV card issuance process, has the ability to undermine the binding of the credential to the person.	...or require the cardholder to provide a primary identity source document (see Section 2.3). If a biometric match is performed, then the type of biometric used for the match shall not be the same as the type of biometric data that is being reset. *If a primary identity source document is provided, then the primary identity source document must match one of the identity source documents previously presented by the cardholder.*	Declined -- The PIV Card counts as 'something you have' since the cardholder provides the card to be reset and the card is returned to the cardholder in a single while-you-wait transaction. Note: As specified in Section 2.5.5 (now Section 2.9.4) a second primary identity source document (besides the PIV Card) is required in order to align with identity proofing requirements at issuance, but it does not need to be the same identity source document as previously presented.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-24	SCA PAC & IC	LaChelle LeVan, Probaris	G	13	638	2.5.6	Suggest clarifying the statement "agencies may revoke certificates corresponding to the option Digital Signature… keys." Section 2.5.2, line 549 states "Revocation of the Digital Signature Key is *only optional* if the PIV Card has been collected and zeroized or destroyed." For clarity, suggest restating the scenario for mandatory digital signature key revocation from Section 2.5.2 in Section 2.5.6.	…agencies may revoke certificates corresponding to the optional Digital Signature and Key Management keys. Revocation of the Digital Signature Key certificate is only optional if the PIV Card has been collected and zeroized or destroyed. Similarly, the Key Management Key certificate should also be revoked if there is risk that the private key was compromised.	Resolved by revised text in Sections 2.9.2 and 2.9.5 (formerly Sections 2.5.2 and 2.5.6). See also NCE-31.
SCA-25	SCA PAC & IC	Bob Dulude, ActivIdentity	E	13	643	2.5.6	The acronym "IIF" still appears	Replace with PII which is used in line 671	Accept use of PII. We will define PII with a reference to OMB M-07-16. Also, delete IIF from the glossary.
SCA-26	SCA PAC & IC	Gilles Lisimaque, IDTP	T	21	862	4.1.2	ISO 7810 does not define anything useful related to card durability. Here is a quote from the standard: 8.7 Durability "Durability of the card is not established in this International Standard. It is based on a mutual agreement between the card purchaser and the supplier." NOTE: ISO/IEC 24789 is now under development and will contain durability tests.	Remove the bullet about ISO/IEC 7810 reference to durability. Add statement: Durability is based on a mutual agreement between the card purchaser and the supplier. Provide an informative reference to ISO/IEC 24789 as being under development.	Resolved by IDTP-10.
SCA-27	SCA PAC & IC	Multiple	G	21	870	4.1.3	Durability and longevity specifications that match the PIV card use cases are needed. NOTE: ISO/IEC 24789 is now under development and will contain durability tests and profiles; this could be used as a model to define profiles that allow PIV card issuers to choose from one or more selected profiles.	NIST should lead an initiative to investigate, find or define an appropriate durability specification and test protocol for PIV cards, including working with card manufacturers and other interested parties.	Noted.
SCA-28	SCA PAC & IC	Gilles Lisimaque, IDTP	E	22	915	4.1.3	The sentence indicates the PIV card may be subject to additional testing but does not say by which entities; is it GSA, NIST, or another entity? What are the possible reasons for such additional tests?	Provide some explanation/guidance about the meaning of the sentence.	Resolved by AI-4 and ES-10.
SCA-29	SCA PAC & IC	Bob Dulude, ActivIdentity	G	22	915	4.1.3	This sentence provides little value without examples.	Remove sentence	Resolved by AI-4 and ES-10.
SCA-30	SCA PAC & IC	Lars Suneborn, HIRSCH	G	23	952	4.1.41	Font size es 8 and 7 points conflict with GSA APL Graphical Personalization Approval Procedure GP 25. Font minimum 10 points.	Align the documents. Update GSA APL to allow less than 10 points.	Out of scope. GSA will be responsible for updating APL.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-31	SCA PAC & IC	LaChelle LeVan, Probaris	G	25	1005	4.1.4.3	The optional requirement for Zone 15F: Color coding for Employee Affiliation contains multiple options which require clarification. Individual PIV cardholders may have more than one of the characteristics which may be identified by color. For example, a PIV cardholder may be both a Contractor and a Foreign National. In addition, the use of Red for emergency response officials is in conflict with Figure 4-4, Section 4.1.5, Table 4-2 and the NIST SP 800-104 recommendations. Directly from NIST SP 800-104, page 3, paragraph 1: "Foreign National color-coding has precedence over Government Employee and Contractor color-coding. Foreign National, Government Employee, and Contractor color-coding have precedence over Emergency Response Official color-coding (this implies that Red will never be visible in Zone 15)." Suggest: 1) adding language to FIPS 201-2 Section 4.4.1.3 to more accurately identify which color codes have preference in situations where a PIV cardholder meets more than one of the criteria for the optional color coding; and 2) Remove the use of Red for Emergency Response Officials designation and relegate this information to the Zone 12F footer as currently specified in the draft.	Zone 15F—Color-Coding for Employee Affiliation. Color-coding may be used for additional identification of employee affiliation (see Section 4.1.5 for Color Representation). If color-coding is used, it shall be used as a background color for Zone 2F (name) as depicted in Figure 4-4. The following color scheme shall be used for the noted categories: + Blue—foreign nationals + Green—contractors. + White - Employees. Foreign National color-coding has precedence over Government Employee and Contractor color-coding. These colors shall be reserved and shall not be employed for other purposes. Also, these colors shall be printed in accordance to the color specifications provided in Section 4.1.5. Zone 15F may be a solid or patterned line at the department or agency's discretion.	1) Resolved by adding the following SP 800-104 precedence text in Section 4.1.4.3: "Foreign National color-coding has precedence over Government Employee and Contractor color-coding." 2) Resolved by removing "Red" and adding "White."
SCA-32	SCA PAC & IC	LaChelle LeVan, Probaris	G	26	1018	4.1.4.3	The optional requirement for Zone 16F: Photo Border for Employee Affiliation contains multiple options which require clarification. Individual PIV cardholders may have more than one of the characteristics which may be identified by color. For example, a PIV cardholder may be both a Contractor and a Foreign National. In addition, the use of Red for emergency response officials is in conflict with Figure 4-4, Section 4.1.5, Table 4-2 and the NIST SP 800-104 recommendations. Directly from NIST SP 800-104, page 3, paragraph 1: "Foreign National color-coding has precedence over Government Employee and Contractor color-coding. Foreign National, Government Employee, and Contractor color-coding have precedence over Emergency Response Official color-coding (this implies that Red will never be visible in Zone 15)."	...shall not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, blue shall be reserved for foreign nationals and green for contractors. Foreign National color-coding has precedence over Government Employee and Contractor color-coding. All other colors may be used at the department or agency's discretion.	Declined precedence requirements only apply to Zone 15F.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-33	SCA PAC & IC	Gilles Lisimaque, IDTP	E	33	1091	Figure 4-6	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and also show the chip in the proper location. Also indicate in a note that the chip is on the front of the card.	Accept.
SCA-34	SCA PAC & IC	Neville Pattinson, Gemalto	T	34,35	1096-1103	4.1.4, Figures 4-7 and 4-8	Contact chip is shown in an incorrect position in Figure 4-7 and Figure 4-8. Chip should be shown in the same position as in FIPS 201-1.	Correct image of the card in Figures 4-7 and 4-8.	Resolved by reverting back to FIPS 201-1, removing references to TSA, DOB, and Gender, adding 'B' to zone numbers. Removed reference to TSA as per resolution on comment number DHS-24.
SCA-35	SCA PAC & IC	Gilles Lisimaque, IDTP	E	34	1096	Figure 4-7	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and also show the chip in the proper location. Also indicate in a note that the chip is on the front of the card.	Accept.
SCA-36	SCA PAC & IC	Gilles Lisimaque, IDTP	E	35	1100	Figure 4-8	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and also show the chip in the proper location. Also indicate in a note that the chip is on the front of the card.	Accept.
SCA-37	SCA PAC & IC	Multiple	G	37	1142	4.1.6.1	The standard should allow PIV issuers to choose an operational biometric authentication method where the reference data is stored in the PIV card. This should allow agencies to choose a given biometric method in their own environment (e.g., for specific constraints such as contactless requirement) without disturbing the global interoperability of the PIV system.	Suggested text to be added after line 1142 as a new bullet: + Data containers reserved for data objects specific to the PIV card issuer (e.g., for operational biometrics).	Declined - See http://www.idmanagement.gov/documents/hspd12_faqs_technical.pdf question 7.
SCA-38	SCA PAC & IC	Gilles Lisimaque, IDTP	E	37	1153	4.1.7	"… operations such as reading …." Technically the card can always read information in its memory, but the privileged operations mentioned here are about a reader trying to access (read) the information.	Suggested to change the sentence as follows: "The PIV Card shall be activated to perform privileged operations such as allowing the reader to access biometric information …."	Resolved by DoD-38.
SCA-39	SCA PAC & IC	Walter Hamilton, IBIA	T	37	1161	4.1.7.1	This section states that "Other card activation mechanisms, only as specified in [SP 800-73], may be implemented and shall be discoverable."	It is recommended that biometric match on card be included as a user-based cardholder activation mechanism and included in a future version of SP 800-73.	Noted see disposition of PB-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-40	SCA PAC & IC	Gilles Lisimaque, IDTP	T	38	1186	4.2	It is perfectly correct to say that the signature adds entropy to the unsigned CHUID, but this is not a good reason to assimilate the signed CHUID into a password because any authenticator has to be kept private. The signed CHUID is a public identifier which can be read over any interface by any reader without the user's knowledge. This paragraph, as written, would tend to suggest that the signed CHUID could be used for authentication. However, the signed CHUID is only an identifier and should be treated as such. It may indeed be good practice to store only a hash value of the CHUID in relying systems, but this section should in no way recommend assimilating into, or using the CHUID, as a password.	Remove the paragraph or replace the whole paragraph with the following: "The CHUID may be read and used by the relying system and should be treated as an identifier. It provides information about the CHUID issuer and cannot be modified or altered because of its digital signature. But even so, the CHUID should not be used as an authenticator as it can be duplicated, cloned or replayed even without the legitimate cardholder's knowledge or consent. It can be used as an index pointer in relying systems; but used alone, should not be considered as an authentication factor regarding the user or his/her card."	Resolved by Cert-73.
SCA-41	SCA PAC & IC	Walter Hamilton, IBIA	T	39	1232	4.3	This section refers to "keys used to establish a secure messaging" which can be performed over the contactless interface.	It is recommended that biometric match on card, when implemented over the contactless interface, require secure messaging to protect the privacy of the contactless transmission of the cardholder's presented template from the reader to the card. It is assumed that such an implementation will be further specified in a special publication.	Out of scope. This is an 800-73 question.
SCA-42	SCA PAC & IC	Gilles Lisimaque, IDTP	E	40	1250	4.3	It is a good thing that the CAK Asymmetric is now a requirement, but there should be a timetable, and/or a migration plan, indicating how agencies which did not have it before will change their cards and systems that use cards.	Suggested to add a note: "As the previous standard did not make this a mandatory key, relying systems must test for the presence of the related certificate and not reject a card as a false PIV card solely due to the absence of this certificate." See also comment 4 about application version discovery.	Resolved by IDTP-19.
SCA-43	SCA PAC & IC	Jason Rosen, NASA	G	39	1251	4.3	The symmetric (secret) card authentication key is optional. Agencies that only support symmetric keys (and do not support asymmetric keys) and do not share the symmetric keys will not be interoperable with other agencies.	NIST should issue guidance on requirements for interoperability for high assurance over the contactless interface apart from using the mandatory Card Authentication Key.	Declined to provide symmetric key only interoperable solution. Key management with symmetric keys is difficult to implement due to key distribution and management across agencies.
SCA-44	SCA PAC & IC	Jason Rosen, NASA	G	41	1276	4.3	FIPS 201-2 should consider a National Security Background investigation conducted at the Secret Level or higher as equivalent to the NACI for identity proofing, at the agency's discretion.	A National Security Background investigation conducted at the Secret Level or higher that is within its valid time period should suffice to issue a PIV or PIV-I card.	Resolved by SCA-9.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-45	SCA PAC & IC	Gilles Lisimaque, IDTP	T	41	1298	4.3	The paragraph about symmetric keys clearly indicates there are commands and containers which are not (and will not be) specified in the FIPS 201 standard. Nevertheless, it should be clearly indicated in the relevant standards which commands, references, container identifiers and so on are available for such additional features. Not mentioning what is reserved for PIV and what is available for additional features is begging for collisions with future updates of the PIV standard that could disrupt previous implementations.	Suggested to modify the last sentence: "This standard does not specify key management protocols or infrastructure requirements, but will provide naming spaces as well as card commands allowing such functions not to compromise this or future versions of this standard due to collisions."	Resolved by IDTP-20.
SCA-46	SCA PAC & IC	Multiple	E	42	1321	4.4	"The facial image is not required to be stored on the card" may be a misleading sentence as the facial image is always stored (printed) on the card. It is also recommended that the facial image be a mandatory data object.	The facial image should be a mandatory data object that is stored in the card; the access control for the facial image should be changed to free-read.	Accept to make facial image a mandatory data element. Decline to change access control rule for facial image.
SCA-47	SCA PAC & IC	Gilles Lisimaque, IDTP	E	42	1335	4.4	"The PIV Card shall not permit exportation of the on-card biometric comparison data." This sentence seems to assume the on-card biometric reference data is different from the biometric data stored in the PIV data object available on the contact interface. If this MUST be the case, this should be explained in more detail.	Indicate that the on-card biometric data should be from a different finger(s) from the finger(s) used for off-card matching.	Declined. Requiring different fingers would present a usability impediment: users would have to remember which fingers to present. On the security side, requiring different fingers would mitigate on-card impostors after they had stolen a cardholder's PIN and off-card templates - the security advantage is not large.
SCA-48	SCA PAC & IC	LaChelle LeVan, Probaris	G	42	1335	4.4	Is there a policy related to the export of the biometric data on the PIV credential to other relying parties?	Provide a reference to clarify biometric export, including use cases and security controls.	Resolved by NIST-72.
SCA-49	SCA PAC & IC	Gilles Lisimaque, IDTP	E	46	1486	4.5.3	"… by means of a firmware-defined adaptation layer …" This layer may not always be implemented in firmware.	Replace the term "firmware-defined" with "middleware."	Resolved by removing "firmware-defined."
SCA-50	SCA PAC & IC	Bob Dulude, ActivIdentity	T	49	1560	5.5	It appears that to revoke a card that both the PIV auth and Card auth certificates need to be revoked. However, either (but not both) auth certificates can be revoked without the card being revoked. See continuation of this comment below (for line 1643).	Clarify the status of the PIV card and the PIV application if one or more authentication certificates are revoked. This is critical for correct authentication processing at the relying party. What is the impact on non-PIV applications, if they exist on the card?	Resolved by AI-21.
SCA-51	SCA PAC & IC	Bob Dulude, ActivIdentity	T	49	1573	5.5.1	The popularity of the http protocol to retrieve PKI related data has resulted in the LDAP protocol being seldom used and of little practical value. The LDAP protocol has already been deprecated in the PIV-I specs.	Require http protocol and allow other optional distribution points to be determined by the implementers.	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-52	SCA PAC & IC	Bob Dulude, ActivIdentity	T	50	1582	5.5.2	HSPD-12 identifies interoperability as a primary goal for the PIV program. The Federal Bridge was implemented to enable interoperability of these PIV cards for PACS and LACS authentication. Nowhere however is there a requirement for SCVP responders to enable the rapid electronic authentication (line 353) goal. This seems to be a glaring oversight. Note that most SCVP responders support both SCVP and OCSP and may be able to use the same URL.	Add a section stating that SCVP responders should be implemented and reference RFC 5055.	Declined. An OCSP responder may either be operated on behalf of the relying party (a locally-trusted OCSP responder) or by (or on behalf of) the CA. In FIPS 201-2, references to OCSP are only for OCSP responders operated by (or on behalf of) the CA. An SCVP server can only be operated on behalf of the relying party. While we do not discourage the deployment and use of SCVP, it is out-of-scope for FIPS 201-2.
SCA-53	SCA PAC & IC	Multiple	G	51	1587	6	PIV cardholder authentication methods shown in Section 6 are incomplete and are only one example of methods that can be used. A special publication could more fully describe PIV cardholder authentication and validation, provide additional details and examples and be updated more easily to reflect new use cases.	Move Section 6 content into a normative special publication that more fully discusses PIV cardholder authentication and validation and provides additional details and examples.	Declined. We believe a faster rate of change of authentication mechanisms might be difficult to follow for product developers, conformance testers, and the relying system applications. Moreover, the approval process for Special Publications is less stringent.
SCA-54	SCA PAC & IC	Lars Suneborn, HIRSCH	G	51	1597	6.1	6.2.2 describes PACS process to read and check verify CHUID signature; 6.2.4.2 describes CAK with Symmetric key, 6.2.6 describes CAK with symmetric key. All are one-factor authentication based on possession. Add a PIN-to-PACS verifier: A knowledge based second factor will strengthen these when the PIN is kept secret. This aligns with common specifications for SCIF access -- i.e., DCID 6/9 JAFAN 6/9 to name a few. In addition FICAM "B" brings in scope functions of physical intrusion detection systems (IDS) which require system based PINs. (See also comment on moving Section 6 to special publication, #53, pg. 51, line 1587, section 6.)	Add: A secret PACS PIN is a knowledge-based factor that may be used in conjunction with possession or biometric-based token as a second factor. This verifier may be required in normal operation of physical intrusion detection functions. The PACS PIN should be encrypted and protected in the PACS and the PIN should be unique to a given user identifier. See also Comment 53.	This comment is out of scope for FIPS 201-2. FIPS 201-2 only addresses authentication mechanisms using the PIV Card. Moreover, these methods are already covered in ICAMSC Federated PACS document.
SCA-55	SCA PAC & IC	Bob Dulude, ActivIdentity	T	52	1643	6.2	In this section it states that the status of the auth certificates is directly tied to the status of all other credential elements held by the card. This raises the question of the status of these other elements if only one auth certificate is revoked. (View this comment in conjunction with the above comment for line 1560.)	Clarify the status of the PIV card and the PIV application if one or more authentication certificates are revoked. This is critical for correct authentication processing at the relying party. What is the impact on non-PIV applications, if they exist on the card? See also Comment 53.	Resolved by AI-21.
SCA-56	SCA PAC & IC	Jason Rosen, NASA	G	52	1650	6.2.1	VIS should not be used as a factor. VIS facilitates the non-electronic use of the PIV card. The only use case for a VIS is to physically look at a person's face and expiration date for authentication. This also affects Table 6.2 on line 1840. (See also comment on moving Section 6 to special publication, #53, pg. 51, line 1587, section 6.)	Clarify that VIS is not an authentication factor. This also affects Table 6.2 on line 1840. See also Comment 53.	Resolved by lowering the assurance level of VIS and by moving the section towards the end. Also, Table 6-2 will be updated accordingly.
SCA-57	SCA PAC & IC	Jason Rosen, NASA	G	54	1687	6.2.2	FIPS 201-2 provides no guidance on protection of devices that perform cryptographic operations and store secrets and/or personal information. Devices that perform cryptographic operations, store secrets and/or personal information should be securely located and protected using approved cryptographic modules.	Either FIPS 201-2 or an associated special publication should include guidance on protection of devices that perform cryptographic operations and store secrets and/or personal information. This guidance must be developed in cooperation with industry. See also Comment 53.	Declined. Such guidance is already provided by other special publications such as SP 800-53.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-58	SCA PAC & IC	Jason Rosen, NASA	G	54	1693	6.2.1	Clarification - An unsigned CHUID alone is not considered one factor. This also affects Table 6.2 on line 1840. (See also comment on moving Section 6 to special publication, #53, pg. 51, line 1587, section 6.)	An unsigned CHUID alone is not considered one factor. This also affects Table 6.2 on line 1840. See also Comment 53.	Out of scope. CHUID must always be signed as per Section 4.2.2 (now Section 4.2.1), and FIPS 201 requires validating the signature. FIPS 201 does not include any authentication mechanisms that allows reading of partial CHUID.
SCA-59	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	54	1693	6.2.2	Conflict with SP 800-73-3 Appendix B. CHUID Signature Check is "Optional" in Figure B-2.	Align FIPS 2- and SP800-73-3 Part 1 Appendix B by removing "Optional" from Figure B-2 diagram. See also Comment 53.	Accept. SP 800-73 Part 1 will be aligned to FIPS 201 after FIPS 201-2 is final. See PB-2.
SCA-60	SCA PAC & IC	Gilles Lisimaqu e, IDTP	T	54	1699	6.2.2	It is not clearly indicated in the section that this mechanism does not provide revocation check of the credential, even when the signature is checked.	Suggest adding a bullet indicating: In order to verify that the card has been revoked, PIV Auth and/or Card Auth certificates need to be checked for revocation, in addition to path validation of the signature of the issuer. See also Comment 53.	Resolved by adding a bullet to Section 6.2.2 (now Section 6.2.5) under characteristics: "Does not provide protection against use of a revoked card."
SCA-61	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	54	1702	6.2.3	Conflict with SP 800-73-3 Appendix B. Signature Check is "Optional" in Figure B-3 BIO Authentication.	Align FIPS 2- and SP800-73-3 Part 1 Appendix B by removing "Optional" from Figure B-3 diagram. See also Comment 53.	Accept. SP800-73 Part 1 will be aligned to FIPS 201 after FIPS 201-2 is final. See PB-2.
SCA-62	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	54	1702	6.2.3	The PIV Card Application hosts the signed fingerprint templates and/or the signed iris image templates. This is a conflict with GSA APL Biometric Reader which has no test requirement for bio signature check.	Align FIPS 201-2 and GSA APL by adding BIO signature check to biometric reader category, or alternatively remove the BIO Reader category. See also Comment 53.	Out of scope. GSA will be responsible for updating APL.
SCA-63	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	54	1702	6.2.3	IRIS process description missing.	Add process description, further clarification around use, and GSA APL category for BIO - IRIS. See also Comment 53.	Declined. The process description in Section 6.2.3 (now Section 6.2.1) applies to all biometrics modalities.
SCA-64	SCA PAC & IC	Gilles Lisimaqu e, IDTP	T	54	1717	6.2.3	It is not clearly indicated in the section that this mechanism does not provide revocation check of the credential, even when the signature is checked.	Suggested adding a bullet indicating: In order to verify that the card has been revoked, PIV Auth and/or Card Auth certificates need to be checked for revocation, in addition to path validation of the signature of the issuer. See also Comment 53.	Resolved by adding a bullet to Section 6.2.3 (now Section 6.2.1) under characteristics: "Does not provide protection against use of a revoked card."
SCA-65	SCA PAC & IC	Jason Rosen, NASA	E	55	1721	6.2.3.1	Clarification of item 1.	Change to : The signed CHUID is read. See also Comment 53.	Declined. CHUID is always signed. PIV data model does not contain unsigned CHUID.
SCA-66	SCA PAC & IC	Gilles Lisimaqu e, IDTP	E	55	1727	6.2.3.1	It should be indicated in this section (maybe in a note applying to all mechanisms) that the sequence proposed is not normative and could be modified for optimization purposes. For example, capturing the individual's live fingerprints earlier in the process allows masking most of the PKI processing time even if he/she is not the legitimate cardholder.	Suggested to add a note attached to bullet 6: "Note: the sequence of operation described in this section may be modified for optimization purposes. For example, capturing the live fingerprint at the beginning of the sequence would shorten the time of the whole verification, as perceived by the user, if other processes (such as PKI processing) can be executed in parallel." See also Comment 53.	Resolved by IDTP-24.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-67	SCA PAC & IC	Bob Dulude, ActivIdentity	T	55	1730	6.2.3.1	Because of the use of a "shall" in line 1720 of this section it implies in line 1730 that the CHUID must be read to retrieve the FASC-N for the comparison check with the FASC-N in the signed biometric data block. Alternatively the FASC-N could be read from the PIV Auth certificate and compared with the FASC-N in the signed biometric data block. There are two advantages to this approach: 1) the PIV auth cert can be tied to the card via a challenge response making it more secure (note both the CHUID and Biometric data block can be copied), and 2) using the CHUID for this process could require reading the full CHUID to check its signature which will significantly increase the processing time and degrade performance. In either case the most likely implementation would have cached the signing certificate.	Since these are presumably examples and not normative prescriptions for how the various authentication mechanisms could be implemented the "shall" in 6.2.3.1 and 6.2.3.2 should be removed. Recognize that the example given represents only one method and that other methods may be applied to achieve the unattended PIV BIO authentication. See also Comment 53.	Resolved by AI-14.
SCA-68	SCA PAC & IC	Bob Dulude, ActivIdentity	E	55	1732	6.2.3.1	In many places in the document the phrase "unique identifier" is used to describe the input to the authorization process (e.g., lines 1695, 1769 and 1814). However, in other places the term FASC-N is used for the same purpose (e.g., line 1732, 1748,1786).	Used the phrase "unique identifier" everywhere for consistency within the document and with the PIV-I specifications as well as in anticipation of future changes within PIV. See also Comment 53.	Resolved by NIST-81.
SCA-69	SCA PAC & IC	Lars Suneborn, HIRSCH	G	55	1734	6.2.3.2	Biometric Authentication Reader Test Approval Procedures for GSA APL inclusion R-BIO-A.16 refers to SP800-78-2 This should be replaced by SP800-78-3.	Update GSA APL "Test Approval Process for Biometric Authentication Reader" section R-BIO-A.16 to SP800-78-3. See also Comment 53.	Out of scope. GSA will be responsible for updating APL.
SCA-70	SCA PAC & IC	Gilles Lisimaque, IDTP	T	55	1738	6.2.3.2	This line states that the PIN entry is verified by the attendant and, as such, implies that this provides "more assurance" than for the BIO alone. It is true that the presence of the attendant does help ensure that there is no fake biometric spoofing as stated later. However, it is inappropriate for an attendant to observe the entry of a cardholder's PIN since it is a secret. Second, entry of a PIN does not prove that the card is genuine as referenced in SP800-116 Section 7.1.7.	Remove or modify the second sentence on line 1738 (third bullet). Consider adding statement that the entire attended operation process is observed by an attendant, as opposed to the value of the PIN entered. See also Comment 53.	Resolved by removing the steps 1-9 (lines 1735-1749) and modifying the sentence as follows. "This authentication mechanism is the same as the unattended biometrics (BIO) authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder."
SCA-71	SCA PAC & IC	Gilles Lisimaque, IDTP	T	56	1751	6.2.3.2	See comment #70 (Page 55, line 1738, section 6.2.3.2).	Change the sentence to read as follows: "This authentication mechanism is similar to the unattended biometrics authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the biometric by the cardholder." See comment 71. See also Comment 53.	Resolved by modifying the sentence as follows. "This authentication mechanism is the same as the unattended biometrics (BIO) authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-72	SCA PAC & IC	LaChelle LeVan, Probaris	T	56	1758	6.2.4.1	6.2.4.1 Authentication with the PIV authentication certificate credential (PKI-AUTH): This sub-section specifies a scenario that is specific to physical access and not logical access for accurate use, particularly in remote access scenarios (as identified in Table 6-3. Authentication for Logical Access). In particular, a reader and associated middleware may read (after PIN entry) more than one certificate from the credential and ensure these certificates are available to applications from the local certificate store. Each PIV required and optional certificate and key pair has 1) policy oids, 2) key usage, and 2) extended key usage (EKU) values which designate the 1) identity level of assurance (per Common), 2) IETF / x509 usage, 3) department or enterprise usage respectively. Suggest modifying both the 6.2.4.1 and 6.2.4.2 sub-sections to clarify the use of PKI for authentication in logical access applications to incorporate the need to incorporate the checks as specified in the language suggestions.	Add: The Policy OID of the certificate presented by the user is validated to meet the policy OIDs (e.g. id-fpki-common-authentication) as specified in Worksheet 9: PIV Authentication Certificate Profile in [PROF]. See also Comment 53.	Resolved by adding a footnote: Path validation should be configured to specify which policy OIDs are trusted. The policy OID for the PIV Authentication certificate is id-fpki-common-authentication. Also, add the same footnote in Section 6.2.4.2 (now Section 6.2.3.2) but replace with "The policy OID for Card Authentication certificate is id-fpki-common-cardAuth."
SCA-73	SCA PAC & IC	LaChelle LeVan, Probaris	T	56	1758	6.2.4.1, 6.2.4.2	There is missing detail on PKI use cases in Section 6. This leads to confusion and mistaken assumptions in requirements for implementations. For example, the use cases in Section 6 are more physical access-oriented and don't map to logical access.	Expand or point to extended use cases that show full range of PKI requirements for both physical and logical access applications. See also Comment 53.	Declined. The use cases are not biased to physical or logical access systems. The missing detail mentioned in the comment is not provided.
SCA-74	SCA PAC & IC	Bob Dulude, ActivIdentity	T	56	1769	6.2.4.1	The Subject Distinguished Name (DN) is typically not required in the implementation of this authentication process. Only the unique identifier is needed.	Change to: The Subject Distinguished Name (DN) and/or unique identifier from the authentication certificate are extracted and passed as input to the access control decision. See also Comment 53.	Resolved by NIST-81.
SCA-75	SCA PAC & IC	Bob Dulude, ActivIdentity	T	56	1772	6.2.4.1	The use of the phrase "online" certificate status checking infrastructure in the first version of this document caused considerable confusion within the industry as many people interpreted this to mean for use in "real time" revocation checking. In fact there must be a certificate status checking infrastructure but it does not have to be "online" at the time the revocation checking is done. The data can in fact be cached.	Remove the word "online" from this sentence. The word "infrastructure" says what needs to be said. See also Comment 53.	Accept to remove the word 'online'.
SCA-76	SCA PAC & IC	Bob Dulude, ActivIdentity	T	56	1789	6.2.4.2	Same comment as #75 above for 56, line 1772, 6.2.4.1	Remove the word "online" from this sentence. The word "infrastructure" says what needs to be said. See also Comment 53.	Accept to remove the word 'online'.
SCA-77	SCA PAC & IC	Lars Suneborn, HIRSCH	E	57	1791	6.2.4.2	Inconsistent with previous Characteristic segments. Does not include + Low resistance to use of unaltered card by non-owner of card	Add: + Low resistance to use of unaltered card by non-owner of card. See also Comment 53.	Resolved by adding the following bullet: + Low resistance to use of unaltered card by non-owner of card.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-78	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	57	1800	6.2.5	Missing specification of unique identifier to output to PACS for authorization (access grant/deny decision).	Add: The unique identifier (i.e., FASC-N or UUID) from the card authentication certificate is extracted and passed as input to the access control decision. See also Comment 53.	Declined. The OCC authentication mechanism is not being specified at this level of detail in FIPS 201-2. Such details will be included in SP 800-73.
SCA-79	SCA PAC & IC	Walter Hamilton , IBIA	E	57	1800	6.2.5	"If" is misspelled	Correct spelling	Accept.
SCA-80	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	57	1800	6.2.5	No category for biometric Match On Card reader on GSA APL.	Add: On-card biometric reader category to GSA APL Evaluation program. See also Comment 53.	Out of scope. GSA will be responsible for updating APL.
SCA-81	SCA PAC & IC	Lars Sunebor n, HIRSCH	E	57	1801	6.2.5	Authentication using On Card biometric match. Missing Characteristic section. Should be formatted as other categories.	Add Characteristic Section. + Digital signature on biometric, which is checked to further strengthen the mechanism + Applicable with contact and contactless based card readers. See also Comment 53.	Resolved by adding the characteristics as follows: - Highly resistant to credential forgery. - Strong resistance to use of unaltered card by non-owner. - Applicable with contact and contactless card readers.
SCA-82	SCA PAC & IC	Gilles Lisimaqu e, IDTP	T	57	1806	6.2.6	Reading the CHUID is useful for two reasons: Obtaining the diversification number used to calculate the correct derived key for the card and to verify the card expiration date in the CHUID. This must be done if the challenge/response used is very basic (as described in this sequence). When using more elaborate authentication protocols which create a session key, it would be much more efficient (as well as more secure) to exchange card information (such as the date) under a session key protection.	Suggested to add a note indicating that "The protocol shown in this section is for information purposes only. Other protocols could be used when exchanging data using a session key." See also Comment 53.	Resolved by IDTP-27.
SCA-83	SCA PAC & IC	Gilles Lisimaqu e, IDTP	T	57	1809	6.2.6	There is no mention at all in this section about key diversification in the card and how the terminal calculates the correct key for the presented card.	Suggested to add a bullet after bullet #3 indicating: "The reader calculates the correct key related to the presented card." See also Comment 53.	Resolved by adding the following text in Section 4.3 (now Section 4.2.2), Symmetric Card Authentication (lines 1293-1298): "If present, the symmetric card authentication key shall be unique for each PIV Card and shall meet the algorithm and key size requirements stated in [SP 800-78]."
SCA-84	SCA PAC & IC	Lars Sunebor n, HIRSCH	E	57	1815	6.2.6.	Authentication using CAK. Asymmetric Key. No Characteristic section. Missing Characteristic section.	Add Characteristic section: + Low resistance to use of unaltered card by non-owner of card + Applicable with contact-based and contactless readers. See also Comment 53.	Resolved by adding the characteristics for symmetric CAK as follows: - Resistant to credential forgery. - Does not provide protection against use of a revoked card. - Low resistance to use of unaltered card by non-owner of card. - Applicable with contact and contactless readers.
SCA-85	SCA PAC & IC	Lars Sunebor n, HIRSCH	G	58	1839	6	Tables 6-2 and 6-3 conflict with SP800-116.	Remove Table 6-2 and Table 6-3 and put these into a special publication that also reconciles the differences. See also Comment 53.	Declined. Our intention is to modify all Special Publications related to PIV to account for changes made in FIPS 201-2 accordingly.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-86	SCA PAC & IC	Gilles Lisimaque, IDTP	T	58	1843	6.3.1 Table 6-2	It is misleading to indicate in this table that VIS or CHUID used alone provide more than "little or no" level of assurance/confidence. In SP800-116, only the combination of VIS and CHUID provides some confidence. (See also comment on moving Section 6 to special publication, #53, pg. 51, line 1587, section 6.)	VIS and CHUID alone should be considered as little or no confidence. Only when used in combination could they provide some confidence. Table should have an additional row with little or no confidence. See also Comment 53.	Resolved by adding a row for LITTLE or NO confidence to include VIS and CHUID. Moreover, we will insert pointer to SP 800-116 for combinations of authentication mechanisms. FIPS 201-2 will say in a footnote: "Combinations of authentication mechanisms are specified in [SP 800-116]."
SCA-87	SCA PAC & IC	Gilles Lisimaque, IDTP	T	58	1845	6.3.1 Table 6-2	It is very misleading to show in this table that VIS and CHUID, taken independently, provide some level of assurance in the identity of the cardholder. (See also comment on moving Section 6 to special publication, #53, pg. 51, line 1587, section 6.)	Add a row at the top of the table labeled as "Little or NO" confidence. Move VIS and CHUID into this row. Also, it may be appropriate to add another column that shows combinations of various of mechanisms. See also Comment 53.	Resolved by adding a row for LITTLE or NO confidence to include VIS and CHUID. Moreover, we will insert pointer to SP 800-116 for combinations of authentication mechanisms. FIPS 201-2 will say in a footnote: "Combinations of authentication mechanisms are specified in [SP 800-116]."
SCA-88	SCA PAC & IC	Lars Suneborn, HIRSCH	G	58	1845	6.3.1	Table 6-2 should consider other authentication factors (e.g., secret PACS PIN or biometrics on PACS). See also other comments on Table 6-2. Authentication factors should be discussed in detail in a special publication.	Add: Possession-based verifiers such as CHUID with signature verification and CAK (Asymmetric and Asymmetric key) may be combined with a secret PACS PIN to achieve Very High Assurance. See also Comment 53.	This comment is out of scope for FIPS 201-2. FIPS 201-2 only addresses authentication mechanisms using PIV Card. Moreover, these methods are already covered in ICAMSC Federated PACS document.
SCA-89	SCA PAC & IC	Gilles Lisimaque, IDTP	T	59	1856	6.3.2 Table 6-3	This table assumes the client (local workstation) on which such verifications are made has not been subject to any kind of attack or malware invasion. This should be mentioned as it is VERY important that the PIN or the biometric data is not captured, cached and replayed in a rogue client.	Add a note under the table: "This table assumes the workstation software and middleware has not been modified or altered by malware." NIST should provide guidance or recommendations on how to protect data contained in elements exchanged today in cleartext between the smart card and the workstation. See also Comment 53.	Resolved by adding the following text to Section 4.4.4, Card Activation Device Requirements. "Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document." Add reference to SP 800-53.
SCA-90	SCA PAC & IC	Gilles Lisimaque, IDTP	E	60	1857	Appendix A	Should indicate this appendix is normative	Add Normative to the appendix.	Resolved by IDTP-31.
SCA-91	SCA PAC & IC	Bob Dulude, ActivIdentity	T	61	1924	A.5	There has been major confusion in the industry regarding the FIPS 201 Evaluation Program over the difference between approved "readers" and "approved authentication systems."	Clarify categories and procedures on the APL and align with real-world system deployments.	Out of scope. APL is the responsibility of GSA.
SCA-92	SCA PAC & IC	Gilles Lisimaque, IDTP	E	62	1934	Appendix B	Should indicate this appendix is informative	Add Informative to the appendix.	Resolved by deleting the appendix as per OPM-6.
SCA-93	SCA PAC & IC	Gilles Lisimaque, IDTP	E	62	1936	Appendix B	This section describes only the NACI process. It could be useful to also describe the CHRC process.	Add a description of the CHRC process to provide a complete example.	Resolved by deleting the appendix as per OPM-6.
SCA-94	SCA PAC & IC	Gilles Lisimaque, IDTP	E	63	1947	Appendix C	Should indicate this appendix is informative	Add Informative to the appendix.	Resolved by deleting Appendix C.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SCA-95	SCA PAC & IC	Gilles Lisimaque, IDTP	E	64	1952	Appendix D	Should indicate this appendix is normative	Add Normative to the appendix.	Resolved by IDTP-35.
SCA-96	SCA PAC & IC	Gilles Lisimaque, IDTP	E	66	1985	Appendix E	Should indicate this appendix is informative	Add Informative to the appendix.	Resolved by IDTP-36.
SCA-97	SCA PAC & IC	Gilles Lisimaque, IDTP	E	68	2079	Appendix E	The definitions of "assurance level" (as shown in table 6-3) and the definition of "identity authentication assurance level" defined in page 68 should be reconciled clearly in the document.	In the whole document, the term "assurance levels" should be explicitly linked to a given authentication mechanism and separated from the "identity assurance level" for a given person.	Resolved by only using 'E-Authentication assurance levels' and 'PIV assurance levels' phrase in Section 6 and appendix.
SCA-98	SCA PAC & IC	Walter Hamilton, IBIA	E	69	2106	Apdx.E	Neither "match on card" nor "on-card biometric comparison" are included in the glossary.	Add "match on card" or "on-card biometric comparison" to the glossary	Accept to add "on-card comparison" with definition: "Comparison of fingerprint data transmitted to the card with reference data previously stored on the card".
SCA-99	SCA PAC & IC	Gilles Lisimaque, IDTP	E	69	2116	Appendix E	Definition of Path Validation should indicate in a note that this process alone does not provide a revocation check of individual credentials.	Include a statement: In addition to this process, a certificate revocation check must be done to make sure that the credential has not been revoked.	Resolved by IDTP-37.
SCA-100	SCA PAC & IC	Gilles Lisimaque, IDTP	T	74	2298	Appendix F	The reference to ISO 7816 without a published date indicates the latest revision of the document is to be used. If this is the case, it should be referenced that SP800-96 used a different reference (ISO/IEC 7816-3:1997) which may not be compatible with the latest version of the ISO 7816-3 protocols. Another option is to update SP800-96 accordingly.	See the next comment (page 76, 2340, Appendix F). No action is needed here if the next comment is addressed	Resolved by IDTP-39.
SCA-101	SCA PAC & IC	Gilles Lisimaque, IDTP	T	76	2340	Appendix F	SP800-96 calls for a deprecated version of ISO/IEC7816-3 (version 1997) which is not compatible with the latest layer definitions of ISO/IEC 7816. This should be indicated in the list of references or SP800-96 should be updated.	Update SP800-96 to use the current version of ISO/IEC 7816-3.	Resolved by IDTP-39.
SCA-102	SCA PAC & IC	Chris Williams, SAIC	G	n/a	n/a	n/a	There is industry interest in adding display technology to the PIV card (e.g., display for one-time passwords). There is also ISO work being done on this topic, SC17/WG4 N2334.	In the development of FIPS 201-2, authors should ensure that FIPS 201-2 language doesn't rule out adding display technology.	Noted.
SCA-103	SCA PAC & IC	LaChelle LeVan, Probaris	T	n/a	n/a	n/a	The entire document needs to be reviewed to clarify the use of the FASC-N vs. other card identifiers (e.g., UUID) for the PIV card.	Add definition section clarifying what are the possible unique identifiers (i.e., FASC-N or UUID) -- i.e., the element that is used as the binding identifier between all data objects in the card.	Resolved by NIST-81.
SIA-1	SIA	PIVWG	G	vi	169	9	"This standard is effective immediately" may not be easy to put into practice. It changes some of the existing practices has impact on other standards (e.g. SP800 series) as well as qualification processes not yet defined. It would be more accurate to indicate this standard replaces and superseedes the previous version.	Suggested sentence: "This standard replaces previous version and will take effect as soon as possible and after all related technical standards have been updated".	Resolved by DoD-3.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-2	SIA	PIVWG	G	2	251	1.3	The sentence indicates this standard may impact existing implementations. This is the case for example for agencies which did not have an asymmetric CAK in the past. Will there be a timetable for migration and indications on how to cope with the transition?	Indicate in a note by adding a sentence a "migration document" will be issued allowing to minimize the impact of such changes.	Resolved by DOJ-1.
SIA-3	SIA	PIVWG	E	2	274	1.3.3	Document defines and uses a new acronym OCC while industry uses the more common phrase "match on card" or MOC. In other places in the document the phrase "cardholder-to-card" or CTC is used (e.g., line 1795) is used.	Establish consistency within the document. Use industry standard MOC terminology.	Resolved by IBIA-1.
SIA-4	SIA	PIVWG	E	5	374	2.1	"An issued credential is not modified, duplicated, or forged". Credentials can be updated by the issuers (e.g. update of the PIK-AUTh certificate when a new key is generated in the card). Suggested to add the word "illegitimately" before modified in the sentence.	Modify sentence: 'An issued credential is not modified by an illegitimate party, duplicated or forged."	Resolved by revising the sentence to "An issued credential is not duplicated or forged, and is not modified by an unauthorized entity."
SIA-5	SIA	PIVWG	E	6	410	2.3	Is the Department of Defense Common Access Card referenced here the transitional card, or the DOD CAC card with a PIV applet onboard, or any of them?	Add PIV Card to list	Resolved by replacing the Common Access Card with the PIV Card on the list.
SIA-6	SIA	PIVWG	G	8	477	2.4	A provision for supplementary credentials bound to mobile devices with Secure Elements different from the PIV Card should be added. This will allow leveraging of the authentication capabilities of mobile devices with non-smart card form factors. For instance this provision may allow email signing on mobile phone.	The FIPS 201 controls for Identity Proofing, Registration and Credential Issuance can be leveraged to issue supplementary credentials. For instance the issuer may require a 1:1 biometric match prior to The Secure Elements used as carriers for supplementary credentials may be subject to FIPS 140-2 policies. The supplementary credentials may be subject to similar usage policies as the PIV credentials. The supplementary credentials may be independently revoked but their life cycle should be bound to the PIV card. i.e. when the PIV card is revoked all credentials are revoked. Their life should not exceed the PIV card life etc.. For instance supplementary credentials' status and validity may be conditioned to the PIV card authentication credential status and validity.	Resolved by AI-2.
SIA-7	SIA	PIVWG	G	8	477	2.4	A provision for the generation of subordinate keys leveraging those existing in a PIV credential would enable additional use cases fro FIPS 201-2	Allow for the generation and support on PIV card of additional subordinated certificates and keys	Declined - See http://www.idmanagement.gov/documents/hspd12_faqs_technical.pdf question 7.
SIA-8	SIA	PIVWG	T	11	583	2.5.4	This paragraph should mention the Security Data Object may also have to be updated as a consequence of other updates.	Add a sentence saying: "The security Data Object in the card shall be updated to reflect any changes made by such modifications".	Resolved by NIST-95.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-9	SIA	PIVWG	E	12	607	2.5.5	Verifying the cardholder biometric stored on the card matches the user may be difficult when the user has forgotten the PIN. This assumes the verification is done based on data stored outside of the card or there is an issuer direct access to the biometric data in the card. Recommendation to what best practice is should be discribed in this process.	Describe the procedure to reset the PIN and verify its biometric information from the card vwhen the PIN has been forgotten by the cardholder and discuss the impact on the number of card authentication factors as a result of this action	Resolved by SCA-22.
SIA-10	SIA	PIVWG	E	13	643	2.5.6	The acronym "IIF" still appears	Replace with PII which is used in line 671	Accept use of PII. We will define PII with a reference to OMB M-07-16. Also, delete IIF from the glossary.
SIA-11	SIA	PIVWG	T	21	862	4.1.2	ISO 7810 does not define anyhting useful related to card durability. Quote from the standard: 8.7 Durability Durability of the card is not established in this International Standard. It is based on a mutual agreement between the card purchaser and the supplier.	Remove the bullet about ISO/IEC 7810 reference to durability. NOTE ISO/IEC 24789 is now under development and will contain durability tests and should be the reference related to durability	Resolved by IDTP-10.
SIA-12	SIA	PIVWG	E	22	915	4.1.3	The sentence indicates the PIV card may be subject to additional testing but does not say by which entities; is it GSA, the Agency, or another entity? What are the possible reasons for such additional tests?	Remove line 915	Resolved by AI-4 and ES-10.
SIA-13	SIA	PIVWG	E	33	1091	Figure 4-6	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and indicate the chip is on the front of the card and show the chip in the proper location as per FIPS 201-1 at the top of the card	Accept.
SIA-14	SIA	PIVWG	E	34	1096	Figure 4-7	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and indicate the chip is on the front of the card and show the chip in the proper location as per FIPS 201-1 at the top of the card	Accept.
SIA-15	SIA	PIVWG	E	35	1100	Figure 4-8	The location of the contact chip should be shown using dashes or a shaded area as the contacts are on the other side of the card.	Represent the chip contact area with dash lines and indicate the chip is on the front of the card and show the chip in the proper location as per FIPS 201-1 at the top of the card	Accept.
SIA-16	SIA	PIVWG	T	37	1139	4.1.6.1	The Card management key should also be an Asymmetric key. Authentication protocols with session key establishment based on Asymmetric keys offer desirable confidentiality properties. For instance , with certain asymmetric key protocols, after a key transport session ends, the knowledge of the management key cannot be used to reveal the transported key. This is not true with symmetric keys.	Allow asymmetric key card management keys.	Resolved by AI-5.
SIA-17	SIA	PIVWG	E	37	1153	4.1.7	"... operations such as reading ...." technically the card can always read information in its memory but the priviledged operations mentionned here is about a reader trying to access (read) the information.	Suggested to change the sentence as follows: "The PIV Card shall be activated to perform privileged operations such as allowing the reader to access biometric information ...."	Resolved by DoD-38.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-18	SIA	PIVWG	T	38	1174	4.1.7.2	When secure messaging is used to perform card management operations, (e.g. SCP03), a PIV card needs a management key set composed of several management keys. The value of each key of the key sets must be globally unique.	Replace with "each PIV card shall contain unique card management keys"	Declined by AI-5.
SIA-19	SIA	PIVWG	T	38	1186	4.2	It is perfectly correct the signature adds entropy to the CHUID itslef but this is not a good reason to assimilate such information to a password (which, as any authenticatior has to be kept private). The signed CHUID is a public identifier which can be read over any interface by any reader without the user's knowledge. This paragraph, as written, would tend to suggest this information can be used for authentication as it is only an identifier and should be treated as such. It may indeed be good parctice to store only a hash value of the CHUID in relying systems, but this section should in no way assimilate, or suggest to use this identifier as a password.	Replace the whole paragraph with the following: "The CHUID is an identifer and not a password. It provides information about the CHUID issuer and cannot be modified or altered thanks to its digital signature. But even so, it cannot be used as an authenitcator as it can be dupplicated, cloned or replayed even without the legitimate cardholder's knowledge or consent. As such it can be used as an index (identifier) in relying systems but used alone, should not be considered as an authentication factor regarding the user or its card."	Resolved by Cert-73.
SIA-20	SIA	PIVWG	T	39	1231	4.3	Once a secure messaging session with card authentication has been set through the contactless interface, (for instance with Opacity ZKM) it should be possible to input the PIN or OCC through that secure channel. After the PIN or Biometric has been verified, the channel is trusted on both sides, and could be used for performing cryptographic operations or reading PIV data elements. This would for instance allow 2- or 3-factor contactless authentication operations. For card management or remote authentication it is desirable to use a mutually authenticated channel. (for instance Opacity Forward secrecy) More generally the protection of PIV card commands with secure messaging obtained from either card authentication or mutual authentication should be possible in contactless or wireless situations.	Enable the full use of a PIV card, including all authentication factors in FIPS 201-2 over a contact and contactless interface and provide a means to accomplish this.	Resolved by AI-7.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-21	SIA	PIVWG	T	41	1282	4.3	The Asymmetric Card Authentication key may also be associated with a card verifiable certificate (CVC) as described in ISO 7816-8 Annex B. A CVC with Elliptic Curve cryptography, can be extremely compact (150-180 bytes for P-256) and allows for rapid authentication through contact or contactless interfaces. A CVC may be signed by the PIV card issuer using a unique key pair including the CVC signing verification public key. The CVC signing vertification key may be itself signed by a digital signatory (PIV signer Dn). The resulting signed object does not need to be stored on the PIV card but it allows relying parties to register and check the status of CVCs signing verification keys. CVC statuses should be indirectly managed. For instance the CVC revocation status should be the status of the Card Authentication key certificate. The above arrangement allows the deployment of CVC-based protocols such as Opacity ZKM and Opacity FS in GICS, and thereby great gains in speed, with the opportunity to secure the contatcless interface with secure messaging..	Mention the optional addition of a Card Verifiable certificate to the Card Authentication key certification data. (See above comment 20)	Resolved by AI-8.
SIA-22	SIA	PIVWG	E	40	1250	4.3	It is a good thing that the CAK Asymmetric is now a requirement but there should be a timetable, and/or a migration plan indicating how agencies which did not have it before will change their cards and systems using cards.	Suggested to add a note: "As the previous standard did not make this a mandatory key, relying systems must test for the presence of the related certificate and not reject as false cards PIV cards without this certificate as not all legacy PIV cards will have a CAK."	Resolved by IDTP-19.
SIA-23	SIA	PIVWG	T	41	1298	4.3	The paragraph about symmetric keys clearly indicates there are commands and containers which are not (and will not be) specified in the FIPS 201 standard. Nevertheless, it should be clearly indicated in the relevant standards which commands, references, container identifiers and so on are available for suchadditional features. Not mentionning what is reserved for PIV and what is available for additiponal features is begging for collisions with future updates of the PIV standard disrupting previous implementations.	Suggested to modify the last sentence: "This standard does not specify key management protocols or infrastructure requirements but will provide naming spaces as well as card commands allowing such functions not to interfere with this standard or its future releases. It is suggested that this provides guidance on establishing a name space that eliminates the possibility of collisions."	Resolved by IDTP-20.
SIA-24	SIA	PIVWG	T	42	1313	4.1.7.2	When secure messaging is used to perform card management operations, (e.g. SCP03), a PIV card needs a management key set composed of several management keys.	Allow the use of "card management key(s)..."	Declined. See AI-5.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-25	SIA	PIVWG	E	42	1321	4.4	"The facial image is not required to be electronically stored on the card" may be a misleading sentence as the facial image is always stored (printed) on the card.	It is suggested "The facial image should be required to be stored electronically in the chip of the card." It is also suggested, "The access control rule for the facial image does not require entering the PIN in order to gain access to the facial image."	Accept to make facial image mandatory. Declined - To maintain privacy control, the cardholder is required to indicate intent of release via PIN entry.
SIA-26	SIA	PIVWG	E	42	1335	4.4	"The PIV Card shall not permit exportation of the on-card biometric comparison data". This sentence seems to assume the on-card biometric reference data is different from the biometric data stored in the PIV data object available on the contact interface. If this MUST be the case, this should be explained in more details.	Indicate if the On-Card-Biometric data must be different from the information stored in the PIV biometric data object. Can NIST clarify if the On-Card Biometric is able to access the Biometric data container?	Accept to clarify in SP 800-76-2. The fingers used for on-card and off-card data may be the same. The on-card and off-card reference data are stored in electronically separate containers on the card according to different syntaxes and data format standards. SP 800-76-2 will clarify this further. Also the on-card biometric data shall never be used to release off-card biometric data.
SIA-27	SIA	PIVWG	E	46	1486	4.5.3	"... by means of a firmware-defined adaptation layer ..." This layer may not always be implemented in firmware.	replace the term "firmware-defined" by "middleware"	Resolved by SCA-49.
SIA-28	SIA	PIVWG	T	49	1560+	5.5	It appears that to revoke a card, both the PIV auth and Card auth certificates need to be revoked. However, either (but not both) auth certificates can be revoked without the card being revoked. See continuation of this comment below (for line 1643)	See comment 33, related to line 1643	Resolved by AI-21.
SIA-29	SIA	PIVWG	T	49	1573	5.5.1	The popularity of the http protocol to retrieve PKI related data has resulted in the LDAP protocol being seldom used and of little practical value. The LDAP protocol has already been deprecated in the PIV-I specs.	Require http protocol only throughout the document and make LDAP optional.	In the second public-comment draft of FIPS 201-2 mention of LDAP will be removed. This will allow any requirements related to LDAP to be specified in the "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" [COMMON], the "Shared Service Provider Repository Service Requirements" [SSP REP], and the "X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program" [PROF], rather than in FIPS 201-2 itself. These documents could then be modified to make LDAP optional, as doing so would not be in contradiction with FIPS 201-2.
SIA-30	SIA	PIVWG	T	50	1582	5.5.2	HSPD-12 identifies interoperability as a primary goal for the PIV program. The Federal Bridge was implemented to enable interoperability of these PIV cards for PACS and LACS authentication. No where however is there a requirement for SCVP responders to enable the rapid electronic authentication (line 353) goal.	Add a section stating that SCVP responders shall be implemented ... Note that most SCVP responders support both SCVP and OCSP and <u>may</u> be able to use the same URI and use RFC 5055	Declined. An OCSP responder may either be operated on behalf of the relying party (a locally-trusted OCSP responder) or by (or on behalf of) the CA. In FIPS 201-2, references to OCSP are only for OCSP responders operated by (or on behalf of) the CA. An SCVP server can only be operated on behalf of the relying party. While we do not discourage the deployment and use of SCVP, it is out-of-scope for FIPS 201-2.
SIA-31	SIA	PIVWG	T	51	1587	6	The authentication methods described are a subset of all possible approaches. In addition new techniques may arise before the timeframe for revision of the standard.	Move all of section 6 to a special publication to allow for innovation and updating of authentication methods.	Declined per SCA-53.
SIA-32	SIA	PIVWG	T	61	1624	A.5	There has been major confusion in the industry regarding the FIPS 201 Evaluation Program over the difference between approved "readers" and "approved authentication systems."	Update the 800 series of Special Publications and help rationalize the categories in the GSA APL.	Out of scope. APL is the responsibility of GSA.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-33	SIA	PIVWG	T	52	1643+	6.2	In this section, it states that the status of the auth certificates is directly tied to the status of all other credential elements held by the card. This raises the question of the status of these other elements if only one auth certificate is revoked. (View this comment in conjunction with the above comment for line 1560+)	Clarify the status of the other credential elements, including other certificates, held by the card if only one authentiation certificate is revoked. This is critical for correct authentication processing at the relying party.	Resolved by AI-21.
SIA-34	SIA	PIVWG	T	54	1699	6.2.2	It is not clearly indicated in the section this mechanism does not provide revocation check of the credential, even when the signature is checked.	Add a bullet indicating: "Does not provide verification of credential revocation against a revocation list published by the issuer." In addition to the process described a revocation check must take place in order for the authentication method to be legitimate.	Resolved by adding a bullet to Section 6.2.2 (now Section 6.2.5) under characteristics: "Does not provide protection against use of a revoked card."
SIA-35	SIA	PIVWG	T	54	1717	6.2.3	It is not clearly indicated in the section this mechanism does not provide revocation check of the credential, even when the signature is checked.	Add a bullet indicating: "Does not provide verification of credential revocation against a revocation list published by the issuer." In addition to the process described a revocation check must take place in order for the authentication method to be legitimate.	Resolved by adding a bullet to Section 6.2.3 (now Section 6.2.1) under characteristics: "Does not provide protection against use of a revoked card."
SIA-36	SIA	PIVWG	T	54	1718	6.2.3	Contactless readers should be authorized to access the biometric information if the transfer is protected with secure messaging with reponse confidentiality obtained after session key agreement with card authentication and PIN verification through secure messaging. (eg. Opacity ZKM, Opacity FS)	Allow access with contactless interface if secure messaging and appropriate authentication protocol steps.	Resolved by AI-7.
SIA-37	SIA	PIVWG	E	55	1727	6.2.3.1	It should be indicated (may be in a note applying to all mechanisms) in this section the sequence proposed is not normative and could be modified for optimization purposes. For example, capturing the individual's live fingerprints earlier in the process allows to mask most of the PKI prosseing time as well as cpaturing the subject fingerprints even if he is not the legitimate cardholder.	Suggested to add a note attached to bullet 6: "Note: the sequence of operation described in this section may be modified for optimization purposes. For example, capturing the live fingerprint at the beginning of the sequence would shorten the time of the whole verification as percived by the user if other processes can be executed in parallel."	Resolved by IDTP-24.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-38	SIA	PIVWG	T	55	1730	6.2.3.1	Because of the use of a "shall" in line 1720 of this section it implies in line 1730 that the CHUID must be read to retrieve the FASC-N for the comparison check with the FASC-N in the signed biometric data block. Alternatively the FASC-N could be read from the PIV Auth certificate and compared with the FASC-N in the signed biometric data block. There are two advantages to this approach: 1) the PIV auth cert can be tied to the card via a challenge response making it more secure (note both the CHUID and Biometric data block can be copied), and 2) using the CHUID for this process could require reading the full CHUID to check its signature which will significantly increase the processing time and degrade performance. In either case the most likely implementation would have cached the signing certificate.	Since these are presumably examples and not normative prescriptions for how the various authentication mechanisms could be implemented the "shall" in 6.2.3.1 and 6.2.3.2 should be removed. (See comment 20)	Resolved by AI-14.
SIA-39	SIA	PIVWG	E	55	1732	6.2.3.1	In many places in the document the phrase "unique identifier" is used to describe the input to the authorization process (e.g., lines 1695, 1769 and 1814). However, in other places the term FASC-N is used for the same purpose (e.g., line 1732, 1748,1786, etc.)	Used the phrase "unique identifier" everywhere for consistency within the document and with the PIV-I specifications as well as in anticipation of future changes within PIV.	Resolved by NIST-81.
SIA-40	SIA	PIVWG	T	55	1738	6.2.3.2	This process does not seem to be in line with SP800-116. It describes here the PIN entry is verified by the attendant and as such provides "more assurance" than for the BIO alone. In SP800-116 this mechanism ends up providing two factors, what you have (the card) and who you are (Bio) but nothing is said about the knowldege factor. If the card is not inspected by the attendant (doing a VIS), the fact the subject enters a PIN is totally irrelevenat as any fake card not even verifying the PIN presented will work as long as the biometyric data is correct (providing only one factor). So either SP800-116 ends up validating the PIN as a factor in the process and not the card, or it is required in here to have a VIS in addition to the BIO alone.	Clarify "view of an attendant" to not imply the witnessing of the PIN value being entered.	Resolved by removing the steps 1-9 (lines 1735-1749) and modifying the sentence as follows. "This authentication mechanism is the same as the unattended biometrics (BIO) authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the biometric by the cardholder."
SIA-41	SIA	PIVWG	T	56	1769	6.2.4.1	The Subject Distinguished Name (DN) is typically not required in the implementation of this authentiation process. Only the unique identifier is needed.	Change language to not require Subject Distinguished Name (DN)	Resolved by NIST-81.
SIA-42	SIA	PIVWG	T	56	1772	6.2.4.1	The use of the phrase "online" certificate status checking infrastructure in the first version of this document caused considerable confusion within the industry as many people interpreted this to mean for use in "real time" revocation checking. In fact, there must be a certificate status checking infrastructure but it does not have to be "online" at the time the revocation checking is done. The data can in fact be cached.	Remove the word "online" from this sentence.	Accept to remove the word 'online'.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-43	SIA	PIVWG	T	56	1775	6.2.4.1	Contactless readers should be authorized to perform PKI-AUTH if the transfer is protected with secure messaging with reponse confidentiality obtained after session key agreement with card authentication and PIN verification thorugh secure messaging. (eg. Opacity ZKM, Opacity FS)	Allow access with contactless interface if secure messaging and appropriate authentication protocol steps. (See comment 20).	Resolved by AI-7.
SIA-44	SIA	PIVWG	T	56	1789	6.2.4.2	same comment as above for line 1772	See above	Accept to remove the word 'online'.
SIA-45	SIA	PIVWG	T	57	1809	6.2.6	There is no mention at all in this section about key diversification in the card and how the terminal calculates the correct key for the card presented.	Suggested to add a bullet after bullet #3 indicating: "The reader calculates the correct key related to the card presented."	Resolved by adding the following text in Section 4.3, Symmetric Card Authentication (lines 1293-1298): "If present, the symmetric card authentication key shall be unique for each PIV Card and shall meet the algorithm and key size requirements stated in [SP 800-78]."
SIA-46	SIA	PIVWG	T	58	1840	6.3.1 Table 6-2	Table 6-2 and 6-3 data	Suggested that tables be updated to provide consistency with perceived stregth of authentication factors and also to be consistent with SP 800-63	Resolved by downgrading CHUID and VIS and by adding LITTLE or NO CONFIDENCE assurance level to Tables 6-2 and 6-3.
SIA-47	SIA	PIVWG	T	58	1840	6.3.1 Table 6-2	Suggest to move this table and associated section to the section 6.1 which addresses already the issue, or to make sure it aligns with section 6.1	Align table with section 6.1 and separate notions of identity assurance from authentication method assurance used (e.g. BIO is less secure than BIO-A, as it is less suceptible to biometirc attacks). Using the term defined in the glossary "identity authentication assurance level" would be a good thing. (See also comment 46)	- Resolved by changing the sentence on line 1624: "Table 6-1 shows the notional relationship between the PIV assurance levels and the M-04-04 E-Authentication assurance levels." - Modify [OMB404] to [OMB0404] everywhere. - Modify [OMB322] to [OMB0322] everywhere. - Declined to move Table 6-2 to Section 6.1 since Table 6-2 is placed correctly after the PIV authentication mechanisms are defined in Section 6.2.
SIA-48	SIA	PIVWG	T	58	1843	6.3.1 Table 6-2	It is misleading to indicate in this table that VIS or CHUID used alone provide more than "LITTLE" level of assurance/confidence. In SP800-116, only the combination of VIS AND CHUID provices some confidence.	VIS and CHUID alone should be considered as Little or no confidence. Only when used in combination they could provide some confidence. (See also comment 46)	Resolved by adding a row for LITTLE or NO confidence to include VIS and CHUID. Moreover, we will insert pointer to SP 800-116 for combinations of authentication mechanisms. FIPS 201-2 will say in a footnote: “Combinations of authentication mechanisms are specified in SP 800-116.”
SIA-49	SIA	PIVWG	T	58	1845	6.3.1 Table 6-2	It is very msileading to show in this table that the BIO-A mechanism provides the same level of assurance than PIK-AUTH, specially when VIS is not perfomed in BIO-A.	Move BIO-A in the same row than BIO unless VIS is part of the process included in BIO-A. (See also comment 46)	Declined. BIO-A offers higher assurance than BIO.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-50	SIA	PIVWG	T	58	1845	6.3.1	In section 6.1The definitions provided by NIST to qualify as a VERY HIGH Confidence level is "*A Very strong degree of assurance in the Identity of the Cardholder*" based on the the strength of the technical mechanisms used to verify that the cardholder is the owner of the PIV Card. In Section 6.3.1 they have listed PKI-AUTH as VERY HIGH confidence with out any way to technically validate that the cardholder is the owner of the PIV Card. The only technical mechanism used in the PKI-AUTH to attempt to bind the user to the card is the PIN number. This is in no way an approved method to provide a VERY HIGH degree of confidence that the Cardholder is the actual owner of the PIV Card. While we feel that PKI-AUTH does provide a higher degree of security above a CHUID and PKI-CAK it certainly does not meet the requirements to qualify as a VERY HIGH Confidence to bind the Cardholder to the PIV Card owner.	Lower the Assurance level of PKI-AUTH to High Confidence. This would also apply to section 6.3.2 for Logical Access (See also comment 46)	Declined. We are consistent with SP 800-63-1, which states that PKI-AUTH is VERY HIGH (LOA 4). See SP 800-63-1, Table B.1.
SIA-51	SIA	PIVWG	T	59	1856	6.3.2 Table 6-3	This table assumes the client (local worksattion) on which such verifications are made has not been subject to any kind of attack or malware invasion. This should be mentionned as it is VERY important the PIN or the Biometric data is not captured, cached and replayed in a rogue client.	Add a note under the table: "This table assumes the workstation software and middleware has not been modified or altered by malware."	Resolved by adding the following text to Section 4.4.4, Card Activation Device Requirements. "Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document." Add reference to SP 800-53.
SIA-52	SIA	PIVWG	E	60	1857	Appendix A	Should indicate this appendix is normative	Add Normative in the appendix itself	Resolved by IDTP-31.
SIA-53	SIA	PIVWG	E	62	1934	Appendix B	Should indicate this appendix is informative	Add Informative in the appendix itself	Resolved by OPM-6.
SIA-54	SIA	PIVWG	E	62	1936	Appendix B	This section describes only the NACI process. It could be useful to also describe the CHRC process.	Add a description of the CHRC process to provide a complete example.	Resolved by OPM-6.
SIA-55	SIA	PIVWG	E	63	1947	Appendix C	Should indicate this appendix is informative	Add Informative in the appendix itself	Resolved by deleting Appendix C.
SIA-56	SIA	PIVWG	E	64	1952	Appendix D	Should indicate this appendix is normative	Add Normative in the appendix itself	Resolved by IDTP-35.
SIA-57	SIA	PIVWG	E	66	1985	Appendix E	Should indicate this appendix is informative	Add Informative in the appendix itself	Resolved by IDTP-36.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SIA-58	SIA	PIVWG	E	68	2079	Appendix E	The definitions of "assurance level" (as shown in table 6-3) and the definition of "identity authentication assurance level" defined in page 68 should be reconciled clearly in the document.	In the whole documents the term "assurance levels" is confusing. Clarification related to assurance levels need to take into account the distinction between identity levels of assurance and level of assurance of a given authentication method.	Resolved by SCA-97.
SIA-59	SIA	PIVWG	E	69	2116	Appendix E	Definition of Path Validation should indicate in a note this process in itslef does not provide at all revocation check of individual credentials.	For clarification it is suggested that it be made clear that this process in itself does not provide revocation check of individual credentials. Also provide reference to RFC 5055.	Resolved by IDTP-37 and SCA-18.
SIA-60	SIA	PIVWG	T	74	2298	Appendix F	The reference to ISO7816 without a published date indicates the latest revision of the document is to be used. If this is the case, it should be indicated SP800-96 used a differnt reference (ISO/IEC 7816-3:1997) which may not be compatible with the latest version of the ISO 7816-3 protocols. Another option is to update SP800-96 accordingly.	See comment 61. Nothing to do here if next comment is addressed	Resolved by IDTP-39.
SIA-61	SIA	PIVWG	T	76	2340	Appendix F	SP800-96 calls for an deprecated version of ISO/IEC7816-3 (version 1997) which is not compatible with the latest layer definitions of ISO/IEC 7816. This should be indicated in this list of references or SP800-96 should be updated.	Update SP800-96 to use the current version of ISO/EC 7186-3	Resolved by IDTP-39.
SICPA-1	SICPA	Mike Walsh	T			4.1.2	The PIV card should contain security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. We strongly recommend the minimum of one such security feature be more than one, as layered security provides the best protection against counterfeiting. Adding micro-taggants to the list of security feature examples would also provide for inclusion of covert markers within optically variable inks, making the card and the ink more secure. Covert micro-taggants/markers typically used in security printing range in size from 35-50 microns in diameter and 8-10 microns thick. Indicia can be printed directly onto the micro-structures (e.g., agency logo or acronym). Markers are identified via special detectors that offer non-destructive analysis of the product. The addition of micro-taggants to optically variable inks will not affect the look or feel of the printed design, but adds an additional level of authentication.	Addition of "micro-taggants" to security features list	Declined. Since the VIS authentication has been downgraded to "Little or No Confidence", the increased cost of additional printed security features would not be justified. Also see KAA-1.
SSA-1	SSA	Matthew	E	12	608-610	2.5.5	The term "issuer" on line 608 could be taken to mean a person playing an issuer role or the agency/system doing the issuing. If one takes the term issuer to mean a person in an issuer role, then they see it as a requirement for in person PIN reset. However, lines 609-611 indicate that in-person appearance is a "more stringent" requirement.	Add language to explicitly clarify that unattended PIN reset, using a fingerprint match, is allowed (or not), under FIPS-201-2. Obviously, exception cases requiring a primary identity document are more difficult to handle in the unattended case.	Resolved by new remote PIN reset procedure.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
SSA-2	SSA	Matthew	T	23	943-951	4.1.4.1	This section correctly clarifies a number of issues with regard to physical printing of the name. However, it does not explicitly relate this to the Name field of the electronic Printed Information Object.	Please relate the requirements in this section to the Name field of the Printed Information Object, either in this standard or a revision to SP800-73.	Resolved. Agreed that this comment is out of scope for FIPS 201 and should be handled in SP 800-73, and/or SP 800-85B. This comment will be forwarded to editors of SP800-73.
SSA-3	SSA	Matthew	G	2	248-249	1.2	Requirements for temporary cards certainly should be in scope for this standard. Given the choice of a personally printed, smart card medium for the credential, the operational realities of running smart card printers for a large volume of cards (large deployments use centralized printing out of necessity), the emphasis on card use in M11-11, and operational availability needs, agencies need direction from NIST on compliant issuance of temporary credentials.	Add a section to this standard covering requirements for issuance of temporary credentials.	Declined. The type of temporary card is at an agency decision.
TRE-1	Treasury	Jennifer Evans	T	iv, vi		9	Make this section and (Section 3 - Explanation) more clear and in synch for the final draft. OMB has released memo M-11-11 related to implementation which would allow more specific information to be placed in these sections. In Section 3, page iv, it states "As promptly as possible, but in no case later than eight months after the date of promulgation, executive departments and agencies are required to implement the standard for identification ..." In Section 9 it states "This standard is effective immediately." Consolidate the correct information and update it in these sections of the document.		Resolved by removing the text in Section 3 of the announcement, Explanation, regarding eight month requirement since this text is from the initial FIPS due to HSPD-12. It does not apply for FIPS 201-2.
TRE-2	Treasury	Jennifer Evans	E	vi	176, 178, 180		Sentences with or without period (.) or period (.) vs. Semi-colon (;) - be consistent throughout document.		Accept.
TRE-3	Treasury	Jennifer Evans	E	viii	TOC	1.3	Should use Title case		Accept.
TRE-4	Treasury	Jennifer Evans	T	2	248, 249		Clarify whether out of scope for the initial issuance of the PIV Card only.		Clarified that requirement for temporary cards (whether new or replacement) is out of scope.
TRE-5	Treasury	Jennifer Evans	E	2	270		PIV Card or PIV card - be consistent throughout the document.		Accept.
TRE-6	Treasury	Jennifer Evans	T	5	372	2.1	Explain why this statement is in the document. " A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential;". You could argue then that if you have multiple corrupt officials it is OK issue a credential. There should be a general statement that addresses issuance of credentials and the authenticity and validity of the issuer.		Resolved by WM-3.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
TRE-7	Treasury	Jennifer Evans	T	8	476-477		Clarify under what conditions an agency would reuse or discard a PIV card.		Resolved by Cert-18.
TRE-8	Treasury	Jennifer Evans	T	9	492-494		Clarify this section. What does lapse mean? Why would you issue a PIV Card if the lapse is 60 days or less? Isn't the purpose of a grace period to not issue another PIV card? For example a seasonal worker.		Resolved by new Grace Period text.
TRE-9	Treasury	Jennifer Evans	T	9	508-509		If the PIV Card must be surrendered during renewal, clarify what the employee/contractor is supposed to use for physical/logical access while waiting (could take weeks) for the new PIV Card.		Resolved by revising the text that the card must be surrendered during the renewal.
TRE-10	Treasury	Jennifer Evans	T	10		2.5.2	Clarify what the employee/contractor is supposed to use for physical/logical access while waiting (could take weeks) for the new PIV Card.		Declined. This is an agency specific policy decision.
TRE-11	Treasury	Jennifer Evans	G	22	901		Opposed to punching hole in card; it's not necessary if in a secure card holder. Also thought that that was one of the mandatory security functions that "no holes" were allowed in a card.		Declined. Punching hole is at agency's discretion.
TRE-12	Treasury	Jennifer Evans	E	23	941		Confirm whether "(dpi)" should be lower case.		Confirmed. dpi is used in lower case.
TRE-13	Treasury	Jennifer Evans	E	36	1107		Clarify whether ('blacK') is correct and explain.		Verified ('blacK') is correct.
TRE-14	Treasury	Jennifer Evans	T	37, 38		4.1.7.1	Passwords have more stringent requirements than this. Should not be able to use repeating digits, sequential digits, etc. Should require changing PIN at least once a year.		Declined. Writing a definitive list of PIN quality specifications is out-of-scope of FIPS 201. Minimum PIN update periods are agency optional policy activities.
TRE-15	Treasury	Jennifer Evans	T	38	1168		Clarify the maximum number of digits required. Used to be 8.		Out of scope. Practically, SP 800-73 limits the PIN to length 8.
TRE-16	Treasury	Jennifer Evans	T	43	1352	4.4.1	Clarify the chain or trust for a contractor that works for several agencies. Also, clarify the specific law requirements for retaining this information/record even after the employee leaves and the card is expired.		Each agency may choose to maintain a chain-of-trust record for the contractor. The chain-of-trust is optional. Each agency has its own set of privacy and data retention policies.
TRE-17	Treasury	Jennifer Evans	E	57	1800	6.2.5	"aIf" typo		Accept.
TRE-18	Treasury	Jennifer Evans	E	59	1855	6.3.2	"PKI-CAC" spacing error		Accept.
TRE-19	Treasury	Jennifer Evans	E	61	1928	A.5	"Products" Capitalization error		Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
TRE-20	Treasury	Jennifer Evans	T	66	1985	E.1	Should correspond to what will be used in the ICAM Lexicon.		Declined. Comment does not address any specific shortcomings with the current set of definitions.
TRE-21	Treasury	Jennifer Evans	E	67	2048		"Enrollment data set" should be Title case.		Accept.
TRE-22	Treasury	Jennifer Evans	T	69	2113		One-to-Many can never be a synonym for "Identification". [INCITS/M1-040211] regardless of your source.		Delete the "one-to-many" entry from the glossary. Also delete "This one-to-many matching is called biometric identification."
TRE-23	Treasury	Jennifer Evans	E	71	2180	E.2	"Card Authentication Key" bold font error		Accept.
TRE-24	Treasury	Jennifer Evans	E	71	2197		Confirm whether "(dpi)" should be lower case.		Resolved by TRE-12.
TTWG-1	TTWG	Debbie Sottile 703-371-7544	T		lines 493-494	2.4.2 Grace Period	As stated in document, "does not" exceed is incorrect.	"In instances where such an interregnum **does** exceed 60 days, a card issuer shall issue the employee or contractor a new PIV Card in a manner consistent with PIV Card Issuance."	Resolved by Cert-20.
TTWG-2	TTWG	Debbie Sottile 703-371-7545	T		line 636-637	2.5.6 PIV Card Termination Requirements	FIPS 201-1 stipulates "within 18 hours" and this has been widely accepted as the parameters by Feds and other entities. Recommend maintaining 18 hour parameter.	"The CA shall be informed and the certificates corresponding to PIV Authentication Key and the asymmetric Card Authentication Key on the PIV Card must be revoked **within 18 hours**."	Resolved by AMAG-5.
TTWG-3	TTWG	Debbie Sottile 703-371-7546	T			4.1.4.3 Optional Items on the Front of the Card	As we know, there are many state, local and private sector emergency responders issuing PIV-I credentials that are using the phrase "Emergency Response Official" already. The old FIPS 201 had the "Federal Emergency Response Official" for the federal side stipulated.	"If used, a department or agency may print "**Federal** Emergency Response Official" as depicted in Figure 4-2, preferably in white lettering on a red background."	Accept and as discussed with FEMA. Modify applicable figures accordingly.
USAB-1	U.S. Access Board	Bruce Bailey	G	Federal Register Notice	N/A	p. 12713, column 3	Preamble makes reference to Section 508 of the American with Disability Act. Section 508 is part of the Rehabilitation Act. The FIPS 201-2 text gets this correct.	Section 4.1.4.3 is added to provide requirements for compliance with Section 508 of the Rehabilitation Act	Noted.
USAB-2	U.S. Access Board	Bruce Bailey	G	21	893-896	4.1.3	Section 508 applies proactively to IT system design and after-the-fact accommodations are not sufficient for 508 compliance except in the case of undue burden (1194.1). A decal is not an appropriate solution as all PIV cards must have a tactile discernable orientation for all users.	Braille embossing or other tactile mark must be required as part of the manufacturing process. Another solution is for all PIV cards to have one notched corner.	Resolved by DoD-32.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
USAB-3	U.S. Access Board	Bruce Bailey	T	26	1033-1035	4.1.4.3	Height of Zone 21F (4.5 mm) while sufficient for a tactile marking, will not accommodate even a single line of Braille.	Zone for 508 decals must either (1) be 10mm in height; or (2) permitted to overlap other zones; or (3) tactile marking must be embossed as part of the manufacturing or printing process.	Resolved by removing reference to Braille in Line 895.
USAB-4	U.S. Access Board	Bruce Bailey	E	22	901 - 905	4.1.3	An opening in the card is an efficient approach to providing orientation by touch and should be emphasized as a sufficient technique for 508 conformance.	Departments and agencies <del>may choose to</del> <ins>are encouraged to</ins> punch an opening in the card body to enable the card to be oriented by touch or to be worn on a lanyard. <ins>It is a 508 requirement that IT systems be tactilely discernable.</ins>	Resolved by DoD-32.
USAB-5	U.S. Access Board	Bruce Bailey	G	34	1096	Figure 4-7	Model language regarding alteration of card suggests that a decal applied in support of 508 requirement might "violates section 499 Title 18 of U.S. Code."	Tactile mark for orientation must be part of the manufacturing process.	Resolved by DoD-32.
USAB-6	U.S. Access Board	Bruce Bailey	E	22	899 & 900	4.1.3	These lines reference modification to card in support of 508. This caveat is missing elsewhere.	See following two comments directly below.	Resolved by DoD-32.
USAB-6.1	U.S. Access Board	Bruce Bailey	E	21	898	4.1.3	see above	"The PIV Card shall not be embossed <ins>except as described in support of the Section 508 requirement</ins>."	Resolved by DoD-32.
USAB-6.2	U.S. Access Board	Bruce Bailey	E	53	1671	6.2.1	see above	"The human guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered in any way <ins>except in support of the Section 508 requirement</ins>."	Resolved by DoD-32.
USACE-1	USACE ESC	Craig Zeigler	G				Remove the -2 from the title "FIPS 201-2". Identify revision date only, e.g., "FIPS 201, Effective Date: XX September 2011". This will allow referencing the document in specifications and standards for PACS and keep it more viable. For example, if we reference FIPS 201-1, but NIST publishes FIPS 201-2, it means we must revise all specs and standards to show the new FIPS. Rather, the specs/standards will remain viable if we can reference a FIPS with a statement such as, "FIPS 201, current revision."		Declined. This is the standard naming convention for FIPS. This naming convention does not preclude other documents from referring to this Standard as "FIPS 201, current revision" or "FIPS 201-2 or as revised."
USACE-2	USACE ESC	Craig Zeigler	E	13	643	2.5.6	Spell-out "IIF". This is the first use of the acronym.		Declined. PII will be used.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
USACE-3	USACE ESC	Craig Zeigler	T	13	665	2.6	Clarify that this requirement applies only to "all executive branch departments and agencies ("agencies") and their contractors that use information technology or that operate websites for purposes of interacting with the public" (Ref: OMB322). DoD PACS are not planned for interaction with the public; therefore, this privacy standard should not apply. Plus, performing PIA's on all PACS would be highly cost prohibitive.		Declined. The material is correct as written. This is a policy question, and the determination is made by the agency privacy official.
USACE-4	USACE ESC	Craig Zeigler	T	16	739	Figure 3.1	Shading doesn't match descriptions in preceding paragraphs. The PIV Front-End block in the notional model should be shaded a color differently than the PIV Subsystem and PIV Relying Subsystem		Resolved by updating the figure and its legend to show 3 different shadings. Also add the word "Subsystem" to "PIV Card Issuance and Management" and "PIV Front-End" figure labels.
USACE-5	USACE ESC	Craig Zeigler	T	18	798	3.1.3	Stating "...access control components typically interface with the card reader, the authorization component, the PIN input device, the biometric reader,..." is misleading. From an electronic security systems (ESS) technical perspective a PACS is an integrated system that includes card readers, authorization components (e.g., database), PIN input devices, biometric readers, local processors, enrollment stations (where database is formed), servers, and monitoring/display workstations.		Declined. Section 3 breaks the PIV System into functional components to accommodate both LACS and PACS environments, which integrated systems are based upon.
USACE-6	USACE ESC	Craig Zeigler	T	36	1125	4.1.6.1	Consideration should be given to specifying only mandatory authentication mechanisms for PIV credentials. Allowing optional data fields has created an environment where cards with various data profiles are fielded, within the same body of credentials, which caused inconsistent performance among PACS.		Both mandatory and optional authentication data objects are present as requested by federal agencies. Only the mandatory data object, however, can achieve interagency interoperable authentication.
USACE-7	USACE ESC	Craig Zeigler	T	38	1186-1187	4.2	Make the requirement mandatory. There is no value in storing a complete CHUID in LACS or PACS.		Declined based on Cert-73, IDTP-18, DOJ-11, ES-31, and DHS-6.
USACE-8	USACE ESC	Craig Zeigler	G			Multiple	Throughout the document, SP 800-76 is referred to for iris image specifications. SP 800-76 doesn't, currently, provide specifications for the capture, handling or storage of iris images. Consider referring to ANSI/INCITS 379 "Iris Image Interchange Format" and/or ISO/IEC 19794-6 ", and/or ANSI/NIST-ITL 1-2007 Parts 1 and 2.		Declined: The iris specifications appear in the second revision of NIST SP 800-76, i.e. 800-76-2, which was published in draft form in 2011, and is expected to be finalized in 2012.
USACE-9	USACE ESC	Craig Zeigler	T				This revision should drive a change to the data retrieval time through the contactless reader interface, currently allowed to be 2 seconds (RE: SP800-96). Recommendation: Require the data retrieval time to be commensurate with proximity technology (800 milliseconds or less).		Out of scope. The recommendation will be considered for SP 800-96.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
USCBP-1	U.S. Customs and Border Protection (CBP)	Identity Mgmt. & Credentialing Branch Chief John Caycedo 202-344-1860	G	N/A			FIPS 201-1 clearly showed that the Enrollment Official begins the chain-of-trust; the new FIPS 201-2 draft does not address who actually begins the chain-of-trust. Why create the companion document SP 800-76-2 instead of incorporating into one easy-to-use publication?	Clearly state who initiates the chain-of-trust now that all PIV issuance appears to be on a system-based operation. And, make sure all information is in one publication (not IFIPS 201-2 and SP 800-76-2).	AMAG-6 reorganizes for clarity. Chain of trust is new in FIPS 201-2. Agency actions and required procedures are specified in FIPS 201-2. This refers to technical specifications for data and equipment appearing in 800-76-2. A new special publication will be created to detail chain-of-trust.
USCBP-2	CBP	John Caycedo 202-344-1860	E	2	245	1.2	Grammar: The word "their' references only people, not entities. Entities should not be personified in a formal document.	Remove "their"; replace with "its" or "the".	Declined. 'Their" may be used to refer to entities.
USCBP-3	CBP	John Caycedo 202-344-1860	E	4	327	1.4	Grammar: The word "their' references only people, not entities. Entities should not be personified in a formal document.	Remove "their"; replace with "its" or "the".	Declined. 'Their" may be used to refer to entities.
USCBP-4	CBP	John Caycedo 202-344-1860	E	8	480	2.4.1	Grammar: The word "their' references only people, not entities. Entities should not be personified in a formal document.	Remove the **second** "their"; replace with "its" or "the". (The first "their" is the correct usage.)	Declined. The second 'their' refers to people.
USCBP-5	CBP	John Caycedo 202-344-1860	E	11	604	2.5.5	Grammar: The noun "cardholder" (singular) and the pronoun "their" (plural) need to agree.	Remove "their"; replace with "his or her".	Resolved by using plural. Change 'cardholder' to 'cardholders'
USCBP-6	CBP	John Caycedo 202-344-1860	E	12	627	2.5.6	Grammar: The noun "employee" (singular) and the pronoun "their" (plural) need to agree.	Remove "their"; replace with "his or her".	Accept.
USCBP-7	CBP	John Caycedo 202-344-1860	E	22	948	4.1.4.1	Grammar: The word "their' references only people, not entities. Entities should not be personified in a formal document.	Remove "their"; replace with "its" or "the".	Resolved by changing the sentence to "The identifiers may be printed on separate lines if each fits on one line."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
USCBP-8	CBP	John Caycedo 202-344-1860	E	24	975	4.1.4.3	Grammar: The word "their' references only people, not entities. Entities should not be personified in a formal document.	Remove "their"; replace with "its" or "the".	Declined. Their could be used to address objects.
USCBP-9	CBP	John Caycedo 202-344-1860	E	50	1589	6	Grammar: The word "their' references only people, not entities.	Remove "their"; replace with "its" or "the".	Declined. Their could be used to address objects.
USCBP-10	CBP	John Caycedo 202-344-1860	E	52	1632 1634 1635	6.1.1	Grammar: Three "theirs" are used. Are you referring to people, processes or entities?	Clarify or remove the word "their".	Declined. Their refers to parties/owners of resources.
USCBP-11	CBP	John Caycedo 202-344-1860	E	63	1950	Appendix C	Grammar: "FIPS 201-2 Card Processes and Their Requirements"	Remove "their" to read: "FIPS 201-2 Card Processes and Requirements"	Resolved by deleting Appendix C.
USCBP-12	CBP	John Caycedo 202-344-1860	E	70	2141	Appendix E	Grammar: their	Replace "their" with "his or her".	Accept.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
USCIS-1	U.S. Citizenship & Immigration Services (USCIS)	Keith Hall	G			General	Current Agency process is to attach a photocopy of a badge to an application for a new account (ex. in Active Directory, for a system, etc.). Rationale: this allows verification that a badge was checked as part of the approval and issuance or granting of rights/privileges to a logical account. A concern arose whether the photocopying of an HSPD-12 badge constitutes a policy violation. Without the photocopying of the badge, it would be difficult to verify after-the-fact whether or not a badge was checked when an account privilege was granted (unless an extremely sophisticated IdM system was developed and all legacy systems/processes are retired). Does the photocopying of an HSPD-12 badge violate FIPS 201-1-Change 1, Page 5, Section 2.1: "An issued credential is not modified, duplicated, or forged"? Under what circumstances is it permitted / disallowed? "The content of this message is mine personally and does not reflect any position of the Government or of DHS." DHS MD Number 4600.1, PERSONAL USE OF GOVERNMENT OFFICE EQUIPMENT, 04/14/2003 Prohibition of ID photocopying doesn't make sense from a security perspective. Rationale: hypothetically, a good telephoto lens snapshot, Photoshopped to the officially published card specification will yield almost a perfect replica of a PIV card. The PIV card specifications are published as examples within the FIPS document itself. The security is really in the smart chip - not the image.specification will yield almost a perfect replica of a PIV card. The PIV card specifications are published as examples within the FIPS document itself. The security is really in the smart chip - not the image.		Photocopying a PIV Card is not the same as duplicating or forging a PIV Card.
Viscount -1	Viscount	Steve Pineau	G			G.	It is our humble opinion that the best endpoint for our clients, including FIPS 201 is to migrate PACS systems to a unified physical/logical access control model. With this architecture (provided in a separate power point and white paper) there are no control panels. FIPS 201 card messages are processed directly on the logical system (active directory, Sun, Oracle etc) the same way a FIPS card can be used to login to a network. The only thing we do with our IP encryption bridge is provide an enabling technology to control doors and security hardware through the IT software. This method is both more secure and faster (no PKI issues) than using panels and much less expensive. The whole FIPS 201 implementation issues in terms of control panels and data formats etc. would have been largely mitigated from the get go if only all systems used this architecture going back 5 years but at least now there is a sensible migration path.		Noted.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
Viscount -2	Viscount	Bill Newill				6.3.1	end of sentence 1 * Replace [period] w/ [comma] * Add: "or in a unified Logical/Physical database environment"		Declined. This section addresses physical access in general whether or not it is unified with logical access.
Viscount -3	Viscount	Bill Newill				6.3.2	end of sentence 1 * Replace [period] w/ [comma] * Add: "and also physical access control resources if in a unified database platform."		Declined. This section addresses logical access in general whether or not it is unified with physical access.
Viscount -4	Viscount	Bill Newill				6.3.2	end of para. 1 * Replace [period] w/ [comma] * Add: "including a physical access control environment (in a unified data base platform)"		Declined. This section addresses logical access in general whether or not it is unified with physical access.
Viscount -5	Viscount	Bill Newill				6.4	(New) * Add: "**PIV Support of 'Cloud' Operation**" "Per the OMB mandate to move IT intelligence to the 'Cloud', IS (Information Systems) are structuring a unified PACS (Physical Access Control Systems) / LACS (Logical Access Control Systems) systems approach with physical security as a 'Cloud' app (application). PIV authentication and key verification should have the option of happening at the system level, instead of with the reader, thereby utilizing system trusted sources for information processing and certificate validation."		Declined. This specific approach is permitted in FIPS 201. FIPS 201 does not discuss specific solutions.
WM-1	Private	Will Mor	T	Various	Various	Various	The terms PIV credential and PIV card are used interchangeably. "Credential" is more appropriate and should be the moniker for the token. The FICAM Roadmap and Guidance document § 4.4.1 defines a credential as being a *card* as well as a password, digitical certificate, et alia. Further, the moniker *PIV credential* better aligns with the dictionary definition for credential.	Refer to the PIV token as a "PIV Credential". If not acceptable, review each instance where PIV Card is used to confirm proper usage.	resolved by replacing "PIV credential" with "PIV card" where appropriate.
WM-2	Private	Will Mor	T	5	362-363	2.1	Clarification. Better defines what is an equivalent to an NACI, and that a **FAVORABLE** NCHC check must be completed.	Bullet (+) number 2 - Change Verbiage to Read: "A credential is issued only after a National Agency Check with Written Inquiries (NACI) or equivalent (as defined by the Office of Personnel Management (OPM)) is initiated, and the favorable completion of an FBI National Criminal History Check (NCHC)."	Declined. Current language is consistent with the Springer Memorandum and M-05-24. Note: According to OPM, NCHC are not adjudicated - the NACI is adjudicated.
WM-3	Private	Will Mor	T	5	372-373	2.1	Clarity: Any official, corrupt or not, should not be able to issued or authorize the issuance of a credential to any one with false (or "incorrecct") identification or to those not entitled.	Bullet (+) number 9 - Change Verbiage to Read: "An official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential."	Declined. Bullet 9 is intended to require separation of duties to prevent a single person from intentionally issuing an incorrect credential. It is not intended to address the possibility that an innocent mistake may occur in the issuance process, as it is impossible to ensure that any process is immune to mistakes.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
WM-5	Private	Will Mori	T	6	377-380	2.2	If FIPS-201-2 is to be the authoritative guidance for PIV cred issuance, it should include such documentation that provides amplifying guidance to PIV cred issuance processes/guidance. Similiarly, OMB memoranda that addresses PIV cred issuance (e.g., M-05-24; M-11-11, et alia) should also be included in an appendix with FIPS-201-2	Include the Springer Memorandum as an appendix to FIPS-201-2.	The Springer Memorandum is likely superseded by OPM's future tiered investigative standard. Memoranda could be amended. Including these memoranda, therefore, is not advisable.
WM-5a	Private	Will Mori	T	6	386-389	2.3	Must have a favorably adjudicated NCHC	(See comment number 2 supra): "Bullet (+) number 2 - Change Verbiage to Read: "A credential is issued only after a National Agency Check with Written Inquiries (NACI) or equivalent (as defined by the Office of Personnel Management (OPM)) is initiated, and the favorable completion of an FBI National Criminal History Check (NCHC).""	Declined. Current language is consistent with the Springer Memorandum and M-05-24. Note: NCHC are not adjudicated - the NACI is adjudicated.
WM-6	Private	Will Mori	T	6	393-437	2.3	Reference the USCIS document I-9 as the authoritative source for ID verification. This is a document that is occasionally updated, where FIPS-201-x is static. By requiring documentation as authorized by USCIS I-9, FIPS-201-x will be more of a dynamic document, and insure compliance with DHS standards for identification documentation.	Verbiage should be replaced by directing use of documentation authorized on USCIS I-9 form.	See Cert-10.
WM-7	Private	Will Mori	T	8	457-460	2.4	Clarify: Removes ambiguity and ensures a proper process is employed	Change to read: "The process shall ensure the initiation of a NACI or equivalent or the confirmation of a completed and successfully adjudicated NACI or equivalent. The process shall also ensure a favorable FBI NCHC is completed before issuing an identity credential. The PIV credential shall be revoked if the results of the investigation so justifies."	Declined. Current language is consistent with the Springer Memorandum and M-05-24. Note: According to OPM, NCHC are not adjudicated - the NACI is adjudicated.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
WM-8	Private	Will Mori	T	8 & 9	479-489	2.4.1	Eliminates a department/agency ability to circumvent FIPS-201 policy and the intent of HSPD-12. For example; NASA issued a PIV credential to BUZZ ALDRIN. "Buzz" is a nickname, not his given name (which is Edwin Eugene Aldrin, Jr.). Further, this opens the gate to Depts/Agencies issuing PIV credentials with variations on the name that does not marry with the identification documentation (birth cert, etc.). Depts/agencies will enable the use of middle names on the PIV credential versus the given name to accommodate preferences versus necessity. This will erode the integrity of the PIV Credential system. The current verbiage in FIPS-201 would authorize the issuance of a PIV credential to Barry Obama “just because” that is the desire of the cardholder, and not because of any safety or security issue(s). I have had requests for a PIV credential being issued to "Sonny" followed by the surname. Sonny is the individual's nickname. As the policy is written, if adopted word-for-word by an agency, "Sonny" could appear on a PIV credential, regardless of what the seed documentation (I-9 documents) reflect.	Change to read: "In exceptionally limited circumstances, Federal employees are permitted to use pseudonyms during the performance of their official duties with the approval of their employing agency. (See, for example, Section 1.2.4 of the Internal Revenue Service Manual, which authorizes approval by an employee's supervisors of the use of a pseudonym to protect the employee's personal safety. Section 1.2.4.6.6 of the Manual provides that employees authorized to use a pseudonym in the course of their official duties will be "given a new ID Card with a new ID number", which will also serve as the employee's building pass). In instances where an agency has formally authorized the use of a pseudonym, the card issuer shall issue a PIV Credential to the employee using the agency-approved employee pseudonym. The issuance of a PIV Credential using a pseudonym shall follow the procedures in PIV Credential Issuance Requirements for employee name changes except that the employee must provide evidence satisfactory to the card issuer that the pseudonym is authorized by the employee's agency. Departments and agencies authorizing the use of pseudonyms on a PIV Credential must establish and officially document justification for the use of pseudonyms. Such justification may only be based upon the safety and security of the individual(s) to whom the PIV Credential is issued, and shall be approved on a case-by-case basis by officially established department and agencies procedures."	Resolved by new text.
WM-9	Private	Will Mori	T	9 & 10	507 - 531	2.5.1	When a PIV credential is being renewed, biometric matching must be preformed on the credential, and not through any DB where the biometric data is stored (given the vulnerabilities of computer networks and storage systems, storing of biometric data is an unwarranted risk that opens the USG to litigation if such privacy data is lost or compromised. Other methods (e.g., on card matching) exist and should be employed for renewals). (see NIST verbiage in section 4.2.1. (Lines 1186-1187) concering a stored CHUID).	Update verbiage to clearly specify the requirement to conduct biometric matching from the valid PIV Credential which is being returned for re-issuance.	Declined. Chain-of-trust, requested by agencies, provides cost savings to agencies by reusing previous enrollment record, and all of the data stored in agency systems is subject to FISMA.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
WM-10	Private	Will Mori	T	10 & 11	564 - 566	2.5.2	Updated biometric data must be captured witih every issuance/reissuance of a PIV Credential. This will ensure an individual's biometric data (to include facial image) is accurate, and up to date, versus someone having a 10-year old picture on their PIV Credential, or changes to other biometric (FP or iris) that could change over time. Recapturing of the biometric data with each issuance (initial or subsquent) to insure currency of attributes, bolstering the integrity of the PIV Credential and the FICAM endeavor.	Delete ability for departments/agencies to use biometric data that (should not be) stored in USG databases. Require new biometrics data be captured upon each issuance of a PIV Credential.	Declined, see the rational of WM-9.
WM-11	Private	Will Mori	T	12	627	2.5.6	As a fiscal and time cost saving measure, Depts/agencies need to be able to transfer PIV Credentials to new contracts (e.g., one contractor loses a contract, but their personnel are hired by the winning contractor). For very large contractors (i.e., United Space Alliance has 10K contractors working at NASA), re-badging staff could be cumbersome, costly and redundant for PIV issuers.	Provide authorization to update PIV record to reflect new employer.	Declined. PIV Cards are issued by the federal government to individuals. In the case of contractors, the PIV card does not identify the contractor's employer.
WM-12	Private	Will Mori	T	23	943	4.1.4.1	The use of a full name is an unwarranted privacy issue. The more data that is on the card face only further enables identity thieves. Use of names other than the given and surname must be optional so that a department/agency can determine whether a FULL name is printed on a card.	Update verbiage to make optional the inclusion of middle name(s) as part of the topology.	As per OMB policy guidance, a legal name as found in the source documents shall be used.
WM-13	Private	Will Mori	T	25	993	4.1.4.3	When a ERO designation is made for a cardholder, the use of zone 9F should be mandatory. This will enable officials to visually determine if an ERO is authorized to be within certain restricted areas during emergency operations (e.g., someone with a fire fighter ERO designation may not be involved in LE operations and would be conspicuous, thus assisting all to identify interlopers). Further, standardized verbiage should be provided by FEMA for various ERO categories (e.g., fire fighter, law enforcement, Senior Official, ERT, et alia) to ensure a thorough understanding and adherence to ERO categorization. Because VIPs/Senior Agency Officials (Dept secretaries, Agency administrators, et al.) may not possess the FEMA required qualifications for a ERO designation, an allowance should be made to enable senior officials to obtain an ERO designation to enable ease of movement into and through restricted areas.	Make zone 9F mandatory when the ERO designation is printed on the PIV Card	Declined as per discussion with FEMA.
WM-14	Private	Will Mori	T	25	998.0	4.1.4.3	The optional use of Zone 12F is provided for in figure 4.1, however, not in this section.	Provide verbiage that reflects agency use of zone 12F for "Agency-specific data" as is provided for in figure 4.1	Declined. Zone 12F is not mentioned in Figure 4-1.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
WM-15	Private	Will Morr	T	25	999	4.1.4.3	Fingerprint minutia (template) should be stored on the card - not a fingerprint	Update verbiage to reflect fingerprint minutia versus fingerprint	Accept to harmonize the fingerprint descriptors as follows. 1. Do not use the word "minutia" because the word "minutia" is too prescriptive, since the specification itself is in NIST SP 800-76-2 and could in-principle change or be extended to include other features extracted from fingers. 2. When "two fingerprints" refer to the card data replace with "two fingerprint templates." 3. When "fingerprints" refers to the full set of fingerprints collected for background check use the phrase "full set of fingerprints."
WM-16	Private	Will Morr	T	36 & 37	1132 & 1141	4.1.6.1	Clarification: The two entries contradict each other	Make data in line 1141 optional. FURTHER, NIST must provide detail for individuals whose FP cannot be captured, and who only have 1 or no iris'	Resolved by NCE-37.
WM-17	Private	Will Morr	T	42	1318	4.4	Fingerprint minutia should be stored on the card - not a fingerprint	Update verbiage to reflect fingerprint minutia versus fingerprint	Replace on line 1322 "Two electronic fingerprints" with "Two fingerprint templates". Replace on line 1132 "Two biometric fingerprints" with "Two fingerprint templates". Replace on line 1347 "fingerprints templates" with "fingerprints" Review all other instances of "fingerprints" and "templates" and "biometric fingerprints" for consistency with this resolution.
WM-18	Private	Will Morr	T	42	1322	4.4	Fingerprint minutia (template) should be stored on the card - not a fingerprint	Update verbiage to reflect fingerprint minutia versus fingerprint	Resolved by WM-17.
WM-19	Private	Will Morr	T	42	1326	4.4	A blind individual who has deteriorated optical orbs from which gathering of iris mapping may be impossible.	Provide alternative to obtaining an IRIS (or retina) map	Resolved by DoD-54, DOT-11, DOT-18, GSA-17, and GSA-27.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
WM-20	Private	Will Morr	T	42	1345 & 1346	4.4.1	When a PIV credential is being renewed, biometric matching must be preformed on the credential, and not through any DB where the biometric data is stored (given the vulnerabilities of computer networks and storage systems, storing of biometric data is an unwarranted risk that opens the USG to litigation if such privacy data is lost or compromised (stolen/lost/compromised biometric data is unrecoverable. There does not exist a method to make a person whole again). Other methods (e.g., on card matching) exist and should be employed for renewals). (see NIST verbiage in section 4.2.1. (Lines 1186-1187) concering a stored CHUID). Further, the risks are greater than the advantages, therefore, it is prudent to **prohibit storage of biometric data** for any longer than required to issue a PIV Credential/Card/Token. This further violates the tenets of the FICAM Roadmap and Guidance Document (v1). Specifically, where the Roadmap discusses, "Increase in protection of personally identifiable information (PII) ..." (p. ii) by the unnecessary retention of PII data, and in § 2.3.1 where it discusses, "... refrain from collecting more information than that which is necessary" (p. 12). The following web site supports the assertion that fingerprint minutia can be used to reconstruct fingerprints: http://biometrics.cse.msu.edu/Publications/SecureBiometrics/RossShahJain_FpImageFromMinutiae_PAMI07.pdf. NIST must remember that most departments & agencies require the PIV Credential to be worn on most external part of clothing and displayed at all times while on the department/agency facility(ies). The full name would be visible by all with whom s/he comes into contact.	Remove all requirements for long-term storage of biometric data. All data should be stored on the credential/card which is the possession/under the control of the cardholder. Compromise of a credential/card may result in the compromise of privacy of one individual. Compromise of a database containing biometeric data for a deparment/agency could result in the compromise of thousands, to hundreds of thousands, to millions of employees (civil servant, military, contractor, visitors (foreign nationals), et al.).	Declined. Requirement for long-term storage of biometric data is removed, however, chain-of-trust, requested by agencies, provides cost savings to agencies by reusing previous enrollment record, and all of the data stored in agency systems is subject to FISMA.
WM-21	Private	Will Morr	T	43	1347	4.4.1	For a blind individual who has deteriorated optical orbs; mapping of the iris(s) may be impossible.	Provide alternative to obtaining an IRIS map	Resolved by DoD-54, DOT-11, DOT-18, GSA-17, and GSA-27.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
WM-22	Private	Will Morr	T	43	1349	4.4.1	When a PIV credential is being renewed, biometric matching must be preformed on the credential, and not through any DB where the biometric data is stored (given the vulnerabilities of computer networks and storage systems, storing of biometric data is an unwarranted risk that opens the USG to litigation if such privacy data is lost or compromised (stolen/lost/compromised biometric data is unrecoverable. There does not exist a method to make a person whole again). Other methods (e.g., on card matching) exist and should be employed for renewals). (see NIST verbiage in section 4.2.1. (Lines 1186-1187) concering a stored CHUID). Further, the risks are greater than the advantages, therefore, it is prudent to prohibit storage of biometric data for any longer than required to issue a PIV Credential/Card/Token.	Remove all requirements for long-term storage of biometric data. All data should be stored on the credential/card which is the possession/under the control of the cardholder. Compromise of a credentilal/card may result in the compromise of privacy of one individual. Compromise of a database containing biometeric data for a deparment/agency could result in the compromise of thousands, to hundreds of thousands, to millions of employees (civil servant, military, contractor, visitors (foreign nationals), et al.).	Declined. Requirement for long-term storage of biometric data is removed, however, chain-of-trust, requested by agencies, provides cost savings to agencies by reusing previous enrollment record, and all of the data stored in agency systems is subject to FISMA.
WM-23	Private	Will Morr	T	43	1386	Fn # 14	Incorrect assumption. Unless NIST is instituting a change with this footnote, a new NCHC is not required. NCHC's are not required if an individual has a current NACI on file (recriprocity included). Fingerprints (or minutia/templates) are only captured for encoding on the PIV credential/card/token.	Delete footnote 14, or update it to agree with supra policy.	Resolved by DoD-54.
WM-24	Private	Will Morr	T	43	1354	4.4.1	Chain of trust cannot be verified simply by having a fingerprint card completed "at a police station." There is no guarantee the FP card was not completed somewhere other than a police station (e.g., at home) nor that the individual who provided the FP's is the individual for whom the credential/card/token will be issued. IF NIST is to authorize such a tack, then specificity must be provided that details how to maintain the chain of trust for such an evolution.	Update verbiage to either exclude the ability to have the FPs taken by other an a USG official; or update to provide detailed guidance on how to maintain chain of trust for the FPs taken by a local police department.	Resolved by removing the example (e.g.) from the text. Note: Extended enrollment should adhere to the same requirements as one-time collection for both 10-prints and 2-prints (for on-card fingerprints) in order to maintain the control objective -- regardless of the method used. (The person who's been checked is the person receiving the card). Extended enrollment can be achieved if the 10 prints are matched with the fingerprints to be stored on-card. Because biometric identification using fingerprints is the primary means for law enforcement checks, agencies shall seek OPM guidance for performing law enforcement checks.
WM-25	Private	Will Morr	T	43	1361	4.4.1	Retention of fingerprints presented unwarranted risks. A new BI is not required if an exsiting NACI (or higher) is on file. Affirmation of identity (which is confirmed through seed documentation (I-9 documents)) is made when the individual again provides the identity documents to the enrollment official.	Correct verbiage to reflect requirement to resubmit ID documentaiton to enrollment official, deleting verbiage concerning repeating a BI	Decline to prohibit agencies from retaining fingerprints. Revised sentence in line 1361 to: "The card issuer need not repeat the identity proofing and registration process."

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
WM-26	Private	Will Mori	T	43	1363 - 1368	4.4.1	The only recriprocity that should be accepted by the gaining agency is that data that is included in the Clearance Verification System. The individual reporting to their new work site should provide their ID documentation (I-9 data), The ID data, coupled with a favorable NACI (or equivalent/higher) in the CVS verifies the individual's identity and permits credential/card/token issuance	Update verbiage to eliminate transfer of data between agencies (how would this be accomplished? Allow the individual to hand-carry their data? FTP? How will the data be secured if electronically transfered? NIST will need to provide standardization of this transfer). The requirement to provide I-9 documentation is upheld with every onboarding process between agencies (i.e., when undergoing onboarding/orientation with the gaining agency, the HR speciallist overseeing the "new hire" onboarding requires the completion of an I-9 and presentation of two-identity documents. The employee can provide the same to the enrollment official who, along with the PIV authorizer, confirms BI status in CVS and executes PIV credential/card/token issuance.	Declined. The chain-of-trust capability has been requested by Federal agencies because the alternative, complete re-enrollment, is time consuming and expensive. Import, export, and data format of chain-of-trust records will be specified in SP 800-156.
WM-27	Private	Will Mori	T	43	1372 - 1373	4.4.1	Definition of ":Bometric Identification" is incorrect. Biometric identification is the process of matching a biometric to an individual. The absence of a biometric identity within the NCHC does not provide "biometric identification".	Correct verbiage to reflect a more precise defintion of biometric identification. Recommend it reflecdt that biometric indentification will take place only when the FBI has FP records of individuals who have been arrested by US LE agencies (inlcude INTERPOL if FBI connectivity to INTERPOL is now available for NCHC queries).	Resolved by TRE-22.
WM-28	Private	Will Mori	T	43	1378 - 1382	4.4.1	A blind individual who has deteriorated optical orbs from which gathering of iris mapping may be impossible.	Provide alternative to obtaining an IRIS map. Facial geometry?	Resolved by DoD-54, DOT-11, DOT-18, GSA-17, and GSA-27.
WM-29	Private	Will Mori	T	44	1394	4.4.1	Fingerprint minutia should be stored on the card - not a fingerprint	Update verbiage to reflect FP minutia or template	Resolved by WM-17.
WM-30	Private	Will Mori	T	59	1855	6.3.2	BIO needs to be part of remote/network system enviroment. This is when authentication of a user is most critical. This may require a department/agency to provide capabilities for challenging BIO data remotely; however, this would be challenged on the PIV credential that was issued to the individual(s). As always, based on a risk-assessment of the IT resources to be accessed. However, as threatcons elevate, challenging an individual's ID becomes more critical. Why would the USG want to authorize remote users to have less authentication of their ID than those who have already been vetted (i.e., authenticated through physical security) by the USG entity?	Recommend a 1:1 requirement for Remote and Network System enviornments. (Remote/Network System Environment must at least as stringent as the Local Workstation Environment)	Declined. SP 800-63-1 does not permit use of biometrics as a token for remote authentication.

Cmt #	Org	POC	Comment Type	Page #	Line #	Section	Comment (Include rationale for comment)	Proposed change	Resolution/Response
WM-31	Private	Will Morr	T	63	1950	C	New biometrics must be captured whenever there is a renewal or reissuance of a PIV credential/card/token. An individual can have significant changes in their appearance or their biometrics (retinal or fingerprints) within a 12-year period. Requiring the capture of new biometrics with each issuance of a PIV credential/card/token will ensure a near 1:1 match to the individual to whom hte card is issued	Delete the authority to maintain biometric data for 12-years, and insert language to require the capture of biometric data from the perspective cardholder with every issuance, and that biometric data (i.e., fingerprint minutia or iris) must be deleted after PIV Credential issuance.	Resolved by deleting Appendix C.

List of Organizations

AI	ActivIdentity (HID Global)
AMAG	AMAG Technology
AUDoD	Australian Department of Defence
B&W	B&W Y12 National Security Complex
Bell	Bell ID
CDC	Centers for Disease Control and Prevention
CDL	Coalition for a Secure Driver's License
Cert	Certipath LLC
DAON	Daon
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DSS	Document Security Systems
ES	Electrosoft Services Inc.
FAA	Federal Aviation Administration
FE	Federal Employee, Jeni Cook
FSATO	Federal Student Air Technology Office
GSA	General Services Administration (Managed Service Office and)
IBIA	International Biometrics & Identification Association
ICAMSC	Federal Identity, Credential, and Access Management Sub-Committee
IDTP	Identity Technology Partners
IGL	InfoGard Laboratories
KAA	Kelly Anderson & Associates
LLNL	Lawrence Livermore National Laboratory
LS3	LS3 Technologies
NASCIO	National Association of State Chief Information Officers
NCE	National Collaborative Enrollment
NGA	National Gallery of Art
NIST	National Institute of Standards and Technology
NNSA	Department of Energy, NNSA Y-12 Site Office
OPM	Office of Personnel Management
PB	Precise Biometrics
SCA	Smart Card Alliance
SIA	Security Industry Association
SICPA	SICPA Holding SA
SSA	Social Security Administration
TRE	Treasury
TTWG	Technology Transition Work Group
USAB	U. S. Access Board
USACE	US Army Corps of Engineers, Electronic Security Center
USCBP	U. S. Customs and Border Protection
USCIS	U.S. Citizenship & Immigration Services
WM	Will Morrison