Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
205	Intercede	2	section 4.2.2 top of page 58 on the November 2020 pdf draft, lines 1800 to 1804	The text below the bold section "PIV Card application administration key" seems to be mixing up concepts that relate to the "PIV card application administration key" and the "Secure Messaging key" - certainly it is at odds with sections 4.2.2.6 and 4.2.2.7	I think this may be a formatting/markup issue, where page 58 intends to list "PIV Card application administration key" and "Secure Messaging key" as 2 separate bold-headed sections to indicate 2 separate keys, but an issue with the markup makes it seem to merge into a single section that looks like it is mixing the 2 different keys together.	Accept	Editorial	Accept - Fixed formatting error
206	Intercede	2	section 4.3.1 "Activation by cardholder" line 2008	Quote - "The PIN should not be easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number or phone number)" This is a very sensible line in its intent, but it is problematic in implementation. Ultimately it is the cardholder that chooses the PIN, although the allowable values is limited by the card itself and the software between the user and the card. The card itself clearly cannot enforce this rule (as it does not know the users SSN or phone number and since these are only examples, there is no concrete rule that it can implement) The software between the user and card (e.g. the card issuance system) - could try to do something to implement this rule, but it is problematic: * it is woolly what the matching rules are/what is allowed or disallowed (e.g. SSN) * in order for software to implement the check of the PIN against this data which is personally identifiable information (PII) either the PIN would need to be sent to the backend system to check it is allowed (bad idea to distribute the PIN), or additional PII (e.g. phone number, SSN) would need to be sent to the client for the check on the client	I believe the intent of this statement is that the cardholder is ultimately responsible (and in fact the only part of the system that can enforce this rule), although as written it implies that it is a problem for software to solve (which as written above could cause more problems than it solves). Therefore I suggest changing to: "The cardholder should not choose a PIN that is easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number or phone number)."	Duplicate	PIV Card	Duplicate of issue # 589
207	XTec, Incorporated	2 = Industry	•Section 4.2.2.3, Line 1866 •Section 6.2.4, Line 2316	Please see attached document	Please see attached document	Declined	Authentication	Decline- Agencies have not identified compelling use cases to retain SYM-CAK. The difficulties of symmetric key management, and the related interagency interoperability challenges, make use of SYM-CAK challenging to meet the goals of PIV.
208	Office of Information & Technology (OI&T), Office of Information Security (OIS)	1 = Federal	line 1379 (page 35)	Reference to “American Association of Motor Vehicle Association’s”	This should likely be “American Association of Motor Vehicle Administrators”	Accept	Editorial	Accept

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
209	Generic Smart Cards LLC	2 - Industry	5.5.3	Unlike logical access, PACS solutions generally leverage a credential identifier from which access privileges and other services are then linked. Having a lightweight revocation solution for PACS that conveys issuer trust status, searchable by credential identifier, would provide many benefits	See Document "FIPS201-3 Contribution Clause 5.5.3 UUID Canceled List v2.pdf" sent with this spreadsheet [FIPS201-3 Contribution Clause 5.5.3 UUID Canceled List v2.pdf](https://github.com/usnistgov/FIPS201/files/5894511/FIPS201-3.Contribution.Clause.5.5.3.UUID.Canceled.List.v2.pdf)	Declined	Authentication	Decline - There is no sufficient advantage to warrant a new requirement on issuers to provide an additional revocation mechanism/status service.
210	NASA	1 - Federal	Sec 2.2 Line 557	The minimum requirement for issuance of a PIV is submission of the investigation and completion of the FBI NCHC, as explained in the following paragraph. These paragraphs need to be modified to address the minimum and address continued eligibility for the PIV credential.	"The minimum requirement for PIV Credential eligibility determination is a completed and favorably adjudicated FBI NCHC and a submitted Tier 1 investigation. Continued PIV eligibility is determined by the completed and favorably adjudicated Tier 1 investigation."	Duplicate	Enrollment	Duplicate of issue #363
211	NASA	1 = Federal	Sec 2.4 Line 600, Sec 2.5 Line 836	"Biometric" is used throughout the document for the purpose of comparison but only fingerprint biometric comparisons are ever detailed as an option (line 600). If the intention is to only allow fingerprint biometric comparison, that needs to be expressely stated. If the intention is to allow fingerprint, iris, or facial image biometric comparison (line 636) that needs to be explained.	Clearly define the use of biometric comparison to either be limited to fingerprint biometric comparison or to allow comparison of all other biometrics (iris, facial image). Recommend allowing comparison of all biometric types captured during enrollments when a biometric comparison is needed.	Accept in Principle	Enrollment	Accept in Principle - Updated text in Section 2.3, clarifies that fingerprints are the only allowed biometric for linking to background investigations. Additional biometrics may be used for other verifications if available.
212	NASA	1 - Federal	Sec 2.7 Line 772	No guidance has been forthcoming from the Department of State and such guidance has not been easily available in the past. Is it the intention of this document for the Department of State to issue guidance, similar to OPM issuing the final credentialing standard, for such issuance? Will the Department of State be establishing a group to support such identity proofing inquiries? Is this specifically for PIV-I credentials or is there an as yet unreleased method for issuing foreign nationals a PIV without an investigation and residency as required in the OPM Final Credentialing Standard?		Noted	Enrollment	Noted - Out of scope for FIPS 201

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
213	NASA	1- Federal	Sec 2.7.1 Line 795	"Requiring the station to be maintained in a controlled-access environment and monitored by staff limits options such as enrollment kits that can be mailed to the applicant or even remotely placed kiosks. Supervised remote should not rely on staff at a location but instead the process to securely access the enrollment service and the pre-registration and sponsorship of the individual to be enrolled. Requiring staff to monitor the equipment does not work for remote areas where population and need for enrollment is greatly reduced. The option to allow a shippable enrollment kit (cameras, readers, etc.) would be useful and the only change to the existing requirements would be the first bullet under supervised remote identity proofing. The recommended change would allow for the current proposed implementation of staffing (maintained in a secure manner) and would also allow options for a kit to be securely shipped to an applicant or even a kiosk to be placed at a specific location. The process for using an enrollment kit could be the following: kit is shipped and tracked by issuer; kit is recevied; enrollment is scheduled; operator and applicant connect	Change the first bullet under supervised remote identity proofing requirements to: "The station SHALL be maintained in a secure manner and SHALL be monitored by an operator while it is being used."	Duplicate	Enrollment	Duplicate of issue #580
214	NASA	1 - Federal	Sec 2.8.2 Line 876	Is NIST proposing a solution for how enrollment records can be shared between organizations so these operations can be accomplished? Currently there is no single location where enrollment records reside or can be bridged (e.g., FPKI bridge, CVS for investigations). Can this be a mandatory item and can this be somehow managed by a central Agency (e.g., DCSA)?		Declined	Enrollment	Decline - The current approach to exchange enrollment record is documented in SP 800-156 (Import/Export of Chain of Trust). NIST has no authority to mandate central storage of enrollment record or require exchange (rather than go through re-enrollment).
215	NASA	1 - Federal	Sec 6.2.5 Line 2341	Use of the CHUID should still be allowed within the authentication perimeter (layered access control). For instance, once I have authenticated to a controlled/limited/exclusion space with PKI I should be able to use CHUID to access areas of equal or lesser security requirements within the perimeter.	Deprecate section 6.2.5, Authentication Using the CHUID but do not remove it. Speficy that use of the CHUID for authentication should only be used after an initial authentication using one of the other approved methods.	Declined	Authentication	Decline - The CHUID authentication mechanism was deprecated in FIPS 201-2 for security reasons, and will be removed from -3 for that reason. We will, however, provide additional considerations and guidance in SP 800-116.
216	NIST, Elaine Barker	1 - Federal	See word.doc attachment	See word.doc attachment	See word.doc attachment [Comments on FIPS 201.docx](https://github.com/usnistgov/FIPS201/files/5894717/Comments.on.FIPS.201.docx)	Partially Accept	Other	Partial Accept - some items incorporated.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
217	NASA	1	2.3	2.3 is vague. Needs further explanation of biometric data and it's use prior to this and the following sections using biometrics.	Further define Biometric Data and is use	Declined	Enrollment	Decline - The current section is clear- currently, biometric data collected for background investigations is limited to a full set of fingerprints.
218	Department of Veteran's Affairs (VA)	1	1. Line 989, Section 2.9.3 PIV Card Activation Reset 2. Line 1040, Section General Computing Platform 3. Line 1075, Section 2.9.4 PIV Card Termination Requirements 4. After line 1530, Table 4-1. Name Examples 5. After line 1530, Table 4-1.		1. Would not refer to this as Card Activation. It is a PIV card PIN and/or data reset. 2. "The operator authenticates the owner of the PIV Card through an independent procedure." Vague wording, would recommend adding examples for clarity. 3. "Per OPM guidance, the Central Verification System (or successor) SHALL be updated to reflect the change in status." Just wanted to comment that this may be difficult for some agencies to implement. CVS can be managed by a different office responsible for adjudications/suitability. If a case management system is not in place, they may not get a notification indicating the user has been terminated or separated from the agency. In which case, the notification and CVS change will have to be a manual data entry. 4. Example column is empty. 5. Page 40, Bottom left, seems to have a formatting issue with a long Contractor name in green.	Accept in Principle	Editorial	Accept in Principle - Sub-bullet 1. Updated wording on PIN reset Sub-bullet 2. Updated wording Sub-bullet 3. Noted Sub-bullet 4. & 5. Examples for names have been updated and formatting corrected

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
219	HID Global	2-Industry	Section 2.6.3 Authentication Using PIV Asymmetric Cryptography	With WebAuthn and FIDO specifications reaching maturity and being available in all major platforms, the opportunity to leverage a widely available mechanism for authentication emerges and we believe there is value on recommending its usage.	Add a section with guidance for using FIDO, for example like this: **6.2.3.x Authentication with a Derived FIDO Credential (FIDO-PK)** A FIDO credential could be created following the guidelines provided in Section 2.10 where a valid PIV card is used establish cardholder identity. The derived FIDO credential is then scoped and stored only by the relying party that would use it for subsequent re-authentication. The following steps SHALL be performed for FIDO-PK: - The relying system issues a `navigator.credentials.get` [WebAuthn](https://www.w3.org/TR/webauthn-2/) request to obtain an identity assertion. It is also possible that the relying party issues directly a lower level `authenticatorGetAssertion` to the authenticator, for example in an embedded system that does not have a WebAuthn API layer. This request includes the relying party id and MAY include a user id. If there is no user id in the request, this means that a FIDO Resident Key is expected to provide both	Declined	Authentication	Decline - Out of scope for FIPS 201-3, but may be addressed in SP 800-157 revision.
220	HID Global	2-Industry	Section: 6.3. PIV Support of Graduated Authentication Assurance Levels	At the beginning of section 6 it is stated that graduated authenticator assurance levels are also applicable to derived PIV credentials, but Section 6.3 only mentions the PIV Credential. It would be useful to include examples of acceptable derived credentials.	Add a Table after current Table 6-1. Acceptable Examples of Derived Credentials for Physical Access; and include for the different PAL an example of a valid derived credential, for example a FIDO Level 2 authenticator with resident keys capabilities. Add a Table after current Table 6-2. Acceptable Examples of Derived Credentials for Logical Access; and include the different authentication assurance levels with examples like accessing a native mobile application or a Web Page in a mobile device as well as a regular desktop through a Web browser.	Declined	Authentication	Decline - This belongs in SP 800-157, not here. Also Table 6.1 has been modified. It no longer references PAL
221	HID Global	2-Industry	Section: 5.5.1 Certificate and CRL Distribution, first paragraph	The Standard requires the use of HTTP. Some may infer that HTTPS is also supported or even preferred. Using HTTPS adds complexity to shared hosting of supporting services so it would be good to clarify if it's indeed included.	Add a phrase to the first paragraph stating if HTTPS is also supported or even encouraged or if it's a deliberate choice to limit the protocol to HTTP.	Declined	Other	Decline - This issued is already covered in RFC 5280.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
222	HID Global	2-Industry	Section 7.2 Second Paragraph	OpenID Connect is a well known federation standard that is worth including in the suggested references.	Extend the last phrase in the second paragraph to read: For example, the information can be presented using technologies defined in [RFC 8485] or [SAML-AC] or [OpenID Connect]. Add the corresponding references to [OpenID Connect Federation](https://openid.net/specs/openid-connect-federation-1_0.html) and [OpenID Connect for Identity Assurance](https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html)	Accept in Principle	PIV Federation	Accept in Principle - Add OIDC4IA.
223	HID Global	2-Industry	Section 2.7.1 Supervised Remote Identity Proofing. Fourth paragraph	FIPS 201 should allow supervised remote identity proofing like SP800-63, at locations that do not provide controlled access; e.g.: the ability to do supervised remote identity proofing from the applicant's home. SP800-63 allows it as long as the remote person supervising the identity proofing can see both the applicant and the hardware used to enroll the applicant, which is something achievable today with the availability of high-quality cameras, high bandwidth and Internet connected devices.	Change the first bullet from "The station SHALL be maintained in a controlled-access environment and SHALL be monitored by staff at the station location while it is being used." into "The station SHALL be monitored by the remote live operator while it is being used by the applicant."	Duplicate	Enrollment	Duplicate of #213/214/580
224	HID Global	2-Industry	Section 4.2 PIV Card Logical Characteristics	Add the ability for a PIV card to optionally support the FIDO2 protocol, that is widely supported by the industry. This would have benefits including: - Such FIDO enabled PIV card would natively work with many applications that don't support PIV today; for example, a PIV cardholder could use the FIDO capability on his PIV card to authenticate to a cloud application on his phone using the NFC antenna embedded in the phone without using a derived credential (while still leveraging the FIPS 140 certification of the PIV card for protection of the crypto materials). - The PIV issuance system could configure the FIDO assertion certificate on the PIV card using the PIV digital signatory so that an Identity Provider could be configured to only accept FIDO credentials issued by the agency or the US Federal government at large. - It would be possible for the PIV PIN and FIDO PIN to be one and the same inside the PIV card so that there is no new PIN management to add for the FIDO part.	Add to the fourth paragraph that states "This Standard also defines optional data elements for the PIV Card data model. These optional data elements include" a bullet saying: - A FIDO2 compliant credential including asymmetric keys, attestation and other data required for FIDO2 compliance	Declined	Derived PIV	Decline - The PIV specifications do not currently prohibit the inclusion of other functionality, like a FIDO applet, on a card. The topic of other authenticators will be covered by a revision to SP 800-157.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
225	DoD	1 - Federal	6. Applicability Line 79	This section leaves open to interpretation whether a physical location can be classifed as a "National Security System". DoD recommends providing clarification.	DoD recommends updating as follows: "This Standard is applicable to identification issued by federal departments and agencies to federal employees and contractors for gaining physical access to federally controlled facilities; and for gaining logical access to federally controlled information systems, except for “national security systems” as defined by 44 U.S.C. 3542(b)(2) and [SP 800-59]."	Declined	Other	Decline - Per FISMA, Federal Information Processing Standards are applicable to non-national security systems. The proposed change would have misrepresented the scope and applicability.
226	DoD	1 - Federal	2.2 Credential Requirement Line 557	Lines 557-559, should reference the Office of Personnel Management (OPM) Credentialing Standards Procedures memorandum, titled “Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials,” dated December 15, 2020. This OPM memorandum includes information that could be considered to the contrary of how Section 2.2 is drafted. For example, in the case of non-citizen U.S. Federal employees hired and working in foreign locations, such as local nationals working at an overseas DoD Installation, a Tier 1 investigation is improbable.	"DoD recommends updating language to: “The minimum requirement for PIV Credential eligibility determination for U.S. nationals worldwide and for non-U.S. nationals at locations within the United States is a completed and favorably adjudicated Tier 1 investigation, formerly called a National Agency Check with Written Inquiries (NACI). The minimum requirement for non-U.S. nationals at locations outside the United States are established in OPM Credentialing Standards for Issuing Personal Identity Verification…"". DoD also recommends adding reference to document (footnote or otherwise)."	Partially Accept	Enrollment	Partial Accept - The final version of FIPS 201-3 includes a reference to the new credentialing standards procedures memo released in 2020. Other recommended changes were not incorporated. As previously noted, the current OPM guidance indicates that a favorably adjudicated Tier 1 investigation is the minimum requirement without exception. In particular, the requirements for non-US citizens has not changed.
227	DoD	1 - Federal	2.2 Credential Requirement Line 564	This section states "once the investigation is completed… report the final eligibility determination to the Central Verification System (or successor). This determination SHALL be record in the PIV enrollment record to reflect PIV eligibility for the PIV cardholder and, if applicable, their enrollment in the Continuous Vetting Program." DoD recommends clarification to better align this section with other language in the document about the PIV enrollment record and clarify that how it is constructed (or stored) is within the Federal PIV issuers purview.	DoD recommends the sentence to updated to the following: "...This determination SHALL be recorded in (or available for) the PIV enrollment record..."	Accept in Principle	Enrollment	Accept in Principle - Text will be updated to clarify the results of investigation should be recorded in enrollment record to reflect PIV eligibility for the card holder

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
228	DoD	1 - Federal	2.6 PIV Enrollment Record Line 642	The draft FIPS 201-3 upgrades the requirements for PIV enrollment record (i.e., chain of trust) from optional to mandatory. At the same time, there remains confusion on the definition of PIV enrollment records vs. PIV accounts. DoD recommends additional clarification. --	"DoD recommends the definitions for PIV enrollment record and PIV account be added to the front of this section. Additionally, DoD recommends an update to those definitions to the following: ""PIV enrollment record is a sequence of related enrollment data sets that can be a specific record or a layer of abstraction for PIV issuers to maintain or assemble when needed to support distribution and auditing. The PIV enrollment record typically contains data collected at each step of the PIV identity proofing, registration, and issuance processes."" ""PIV account is the logical record containing credentialing information for a given PIV cardholder. It is not directly related to PIV enrollment records, but nomenclature to describe system/application accounts supported by PIV authentication. It could additionally be related to an account maintained in an Agency's Identity Federation Service Provider to support federated authentication transactions."""	Partially Accept	Enrollment	Partially Accept - Add text indicating that the PIV enrollment record may be maintained across multiple, distributed systems. It is noted that the PIV enrollment record **would** be part of the logical PIV Identity Account. However, some of those records may be stored in different systems (e.g., CMS vs. enterprise IDMS).
229	DoD	1 - Federal	2.6 PIV Enrollment Record Line 642	It is DoD's understanding that NIST's intent for the PIV enrollment record is to identify items that could be included but leave most of implementation to Federal PIV issuers. DoD recommends adding specific language to this section to provide clarification and to emphasize this intention.	DoD recommends the following be added to this section, "As long as data can be retrieved when needed by the PIV issuer, then there is no requirement for data that may reside in other authoritative system to be duplicated in the PIV issuance system."	Declined	Enrollment	Decline - While we agree with the point that the commenter is making, we believe the current text allows this. In addition, #228 will add text clarifying that the PIV enrollment record may be stored in different places.
230	DoD	1 - Federal	2.6 PIV Enrollment Record Line 642	It is DoD's understanding that NIST's intent for the PIV enrollment record is to identify items that could be included but leave most of implementation to Federal PIV issuers. The SHALL requirements for the PIV enrollment record are spread across the document. DoD recommends providing all SHALL requirements for the PIV enrollment records in this section. This will ensure PIV issuers can clearly identify the requirements that must be implemented (SHALL) vs. the ones that SHOULD or COULD be implemented.	"DoD recommends that this section include all SHALL requirements for the PIV enrollment records. Our review identified the following items: * Line 566 * Line 938	Declined	Enrollment	Decline - Different parts of the document deal with different topics. The SHALL requirements are defined in the appropriate areas for clarity

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
231	DoD	1 - Federal	PIV ID Proofing Line 718	This section states "When they are available, cryptographic security features SHOULD be used to validate evidence." DoD recommends providing clarification on meaning or intent, as it is currently unclear what "cryptographic security feature" is intended to cover.	"DoD recommends clearly defining cryptographic security features by adding ""A cryptographic security feature could include, but is not limited to PKI mutual authentication, MRZ signature validation of passports,…"" or other relevant examples. "	Accept in Principle	Enrollment	Accept in Principle - Document update clarifies the intent- namely that evidence that is digitally signed should be cryptographically verified (e.g., e-passports).
232	DoD	1 - Federal	PIV Identity Proofing and Registration Requirements Line 731	This section creates a new requirement for driver licenses used for identity proofing be REAL ID Act compliant. There are serveal mitigating factors for PIV card issuance, including that PIV card applicants must present a secondary ID proofing document, complete a FBI records check, and complete background investigation. Many U.S. states continue to issue both REAL ID Act compliant and non-compliant ID cards. Given scope/applicability of REAL ID Act and existing mitigating factors, DoD recommends against this requirement.	DoD recommends NIST remove the requirement for a REAL ID Act compliant ID cards in the ID proofing process.	Duplicate	Enrollment	Duplicate of Issue #376:
233	DoD	1 - Federal	Section 2.9.1 Line 922 Section 2.9.4 Line 1071	This revision appears to allow certificate to not be revoked if the PIV is collected and destroyed by the card issuer. While destruction of the PIV cards ensures loss of private keys, it does not address potential user behavior issues with email clients (e.g., potential for an unrevoked public key from a collected/destroyed PIV to be available for use in encryption transactions) and confusion (potential for user to recover an unrevoked encryption certificate for a destroyed PIV and continue to use it) when it comes to encryption keys.	DoD recommends a 4th item be added to the revocation process to ensure there are no user behavior issues: "Even if the PIV card was collected and destroyed, the certificate corresponding to the key management key SHALL be revoked, if the key management key is present."	Declined	Other	Decline - After reviewing the existing language in the working draft, we do not believe any change is needed. It is not necessary or desirable to revoke the KMK in all reissuance scenarios. If the KMK certificate is still valid, it can restored from escrow and placed on the new card. It is arguably desirable to revoke the KMK certificate when an employee is terminated, or if the KMK is rekeyed, but that is scenario-specific and nothing in FIPS 201 would preclude that.
234	DoD	1 - Federal	2.9.4 PIV Card Termination Requirements Line 922	Update this section to provide consistency between this section and lines 1085-1086.	DoD recommends adding the following to this section, "In addition, the PIV Card termination procedures SHALL ensure all derived PIV credentials bound to the PIV account are invalidated as specified in Section 2.10.2."	Declined	Derived PIV	Decline - If the reference is to section 2.9.4 the existing text is already in that section, and if it's in 2.9.1, derived PIV termination should not be required on PIV reissuance.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
235	DoD	1 - Federal	2.9.2 PIV Card Post-Issuance Update Requirements Line 974	This section requires remote update of PIVs be conducted over mutually authenticated communication between the issuance infrastructure, user's web browser, and user's PIV. DoD has seen significant dropped transactions and errors in our remote update capability implementing a similar requirement. DoD is migrating to a solution that will allow more transactions to be conducted successfully and still provide a secure mechanism. DoD recommends adding language to cover DoD's emerging post-issuance implementation, which DoD believes provides sufficient mechanism to perform those transactions securely while decreasing failures.	DoD recommends adding the following to this section: "Remote post-issuance updates are sufficiently secure when performed over a server-side only TLS session used in conjunction with the Global Platform Secure (GP) channel where the keys used to establish the GP channel are known only to the issuer and are housed in a FIPS 140 Level 3 device."	Declined	PIV Card	Decline - The existing text does not require TLS, or any other particular protocol. What is describe by the commenter would satisfy the existing requirements in Section 2.9.2.
236	DoD	1 - Federal	2.9.3 PIV Card Activation Reset Line 1036	This section establishes a requirement for PIVs that support OCC biometric comparison needing to do more to reset a PIN than successfully compare the biometrics. It is unclear what other requirements (i.e., connected to issuer operator and issuance operator authenticates the owner of PIV) must be met in this scenario and what specific risk is attempting to be mitigated.	"DoD recommends NIST add clarity to this section about PIN resets by identifying two specific PIN reset function: 1) ""PIN reset to an unlocked/blocked PIN in which the user knows the PIN or leverages the OCC biometric comparison. This should not require connection to issuance infrastructure."" 2) ""PIN reset to a locked/block PIN which fits into the current language in this section."" "	Accept in Principle	PIV Card	Accept in Principle - Document text was updated to describe how PIN resets can be accomplished using OCC.
237	DoD	1 - Federal	2.10.1 Line 1111	This Section requires the issuer of the PIV card and of a derived credential be one and the same entity; this definition is too narrow to account for Agencies where the issuers of derived credentials are not the organization that manages the PIV issuance. (REF: The "[d]erived PIV credentials SHALL be bound to the cardholder's PIV account only by the organization that manages that PIV account", and the binding is described as follows, "[i]ssuance of a derived PIV credential is an instance of the post-enrollment binding".)	"DoD recommends changing 1111-1113 as follows, ""Derived PIV credentials SHALL be bound to the cardholder's PIV account only by the organization that manages that PIV account life-cycle management bound to the cardholder's PIV account or eligibility.""""	Accept in Principle	Derived PIV	Accept in Principle - Text was clarified to show that the if the issuing department or agency relies on shared services for portions of the PIV card or Derived PIV credential issuance process, it is the responsibility of the issuing department or agency to ensure that all credentials and IDMS records are properly maintained throughout the PIV lifecycle.
238	DoD	1 - Federal	4.1.4.1 Mandatory Items on the Front of the PIV Card	DoD requests that NIST add additional language to provide acceptable alternative approaches for Zone 2F: Name.	DoD recommends adding the following to this section: "Line 1 contains Last Name only, using 10pt Arial Bold. If is is too long, the font size is lowered until it does fit. Line 2 contains First Name, Middle Name, Suffix. If it is too long, the Middle Name is reduced to Middle Initial. If it is still too long, font size is lowered until it does fit. 7pt is the lowest the font size used."	Declined	PIV Card	Decline - What is described by the commenter is already allowed by the existing language.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
239	DoD	1 - Federal	4.2.2.1 PIV Authentication Key Line 1836 4.2.4 PIV Unique Identifiers Line 1969	It has become more and more difficult to support authentication interoperability between different federal agency PIV cards as many applications use User Principal Names (UPNs) as a mechanism to provision and manage accounts. Some Federal agencies implement UPNs that are constructed as e-mail addresses while other use random agency specific identifiers. This does not guarantee uniqueness nor decrease the possibility of duplicates. Additionally, there is no federal-wide requirement for all federal agencies to maintain a identity service provider (IdP) and until such is implemented federal-wide, these interoperability challenges need to be addressed through other mechanisms . Positive adjudication of this comment will significant enhance interoperability (for example, this will aid DoD-VA interoperability and onboarding new federal entities to the Federal Electronic Health Record system).	"DoD recommends adding as a mandatory element to the PIV authentication certificate a UPN in the Subject Alternate Name field that conforms with an existing FIPS 201/SP 800-73 attributes (i.e., the last 16 digits of the Federal Agency Smart Card Number (FASCN), i.e., cardholder specific identifier). The construction of the UPN should be the last 16 digits of the FASCN@federal agency abbreviation (e.g., last 16 digits of FACSN@mil or last 16 digits of FASCN@va). "	Declined	PIV Federation	Decline - NIST does not recommend a unique person identifier as a mandatory element in the Subject Alternate Name field. The use of federation may address concerns identifying users across departments and agencies.
240	DoD	1 - Federal	4.3.1 Activation by Cardholder Line 2008	"This new requirement seems to expect the PIV card (and/or PIV issuance system) to ensure the user does not select various PIN combinations. Meeting this mandate would require the development of a new on-card capability and FIPS 140 re-certification. Additionally, the current safeguards appear to be enough to mitigate this perceived risk for a credential used for UNCLASSIFIED/CUI material. The knowledge about the PIN should be that of the PIV cardholder and the actual card. There are a combination of factors (e.g., the length of the PIN, there is a three failed PIN counter, and physical hardware token) that go into meeting the FIPS 140 1:1M probability of an adversary selecting an accurate PIN. As such, it is difficult to understand how this requirement (implement on the card or within the issuance system) would significantly change this equation and those layered security techniques. "	DoD recommends the requirement be removed or made optional.	Duplicate	PIV Card	Duplicate of issue #589

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
241	DoD	1 - Federal	5.2.1 Line 2080	While DoD agrees with the removal of the term "legacy PKI" from FIPS-201, as currently written, FIPS-201 does not accurately address the distinction between Federal department and agency PKIs that are cross-certified with the Federal PKI and those that are operated under the Common Policy itself. Cross certification happens after the two PKIs are deemed comparable, but asserting a policy OID means that the certificate fully meets the requirements. DoD recommends incorporating language to support interoperability while maintaining the sovereignty of department and agency PKIs.	DoD recommends replacing the first sentence with the following: "The required contents of X.509 certificates associated with PIV private keys are based on [PROF]. The relationship is described below for certificates issued under [COMMON], and is described in Section 5.4 for certificates issued by department and agency PKIs that operate under department and agency specific Certificate Policies."	Partially Accept	Other	Partially Accept - It is acceptable to cross-certify PKI with certificate mapping but this allowance is deprecated in this version of the Standard and subsequently removed in next version of Standard. Per discussion with FPKI, this should be address in other ways than putting into the more restrictive standard. Options, for example are a PA policy memo, or possibly updating the certificate profiles to resolve the issue, and at the same time provide greater flexibility going forward.
242	DoD	1 - Federal	5.4 Line 2111	"While DoD agrees with the removal of the term ""legacy PKI"" from FIPS-201, as currently written, FIPS-201 does not accurately address the distinction between Federal department and agency PKIs that are cross-certified with the Federal PKI and those that are operated under the Common Policy itself. Cross certification happens after the two PKIs are deemed comparable, but asserting a policy OID means that the certificate fully meets the requirements. DoD recommends incorporating language to support interoperability while maintaining the sovereignty of department and agency PKIs. Specifically, DoD recommends continuation of the existing requirement that PIV-Authentication certificates assert the fpki-common-authentication policy, but not to add a new requirement for asserting common policy OIDs in signature and key management certificates."	"DoD recommends replacing the current text with the following: 5.4 Agency PKIs Note: this section was formerly entitled ""Legacy PKIs."" Departments and agencies that operate their own agency CAs MAY specify their own policy OIDs in lieu of or in addition to [COMMON] policies in certificates associated with private keys for Digital Signing and Key Management certificates provided that the agency PKI is cross certified with the Federal Bridge CA or Federal Common Policy CA and the asserted agency policy OIDs map to the [COMMON] policy OIDs specified in 5.2.1."	Duplicate	Other	Duplicate of issue #241
243	DoD	1 - Federal	5.5 Line 2121	Does the specification of HTTP for publishing CA certificates preclude the usage of HTTPS? Considering RFC 5280, it probably should.	Suggest the following text be added, "the usage of HTTPS for publishing CA certificates be prohibited in this standard to avoid the issues specified in Section 8 of RFC 5280, one example of which is "relying parties ... MUST be prepared for the possibility that this will result in unbounded recursion."	Declined	Other	Decline - FIPS 201 specifies that HTTP be used, and is now silent on other protocols. As the commenter noted, RFC 5280 has additional guidance on this topic.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
244	DoD	1 - Federal	5.5.1 Line 2132	Does the specification of HTTP for publishing CA certificates preclude the usage of HTTPS? Considering RFC 5280, it probably should.	Suggest the following text be added, "the usage of HTTPS for publishing CA certificates be prohibited in this standard to avoid the issues specified in Section 8 of RFC 5280, one example of which is "relying parties ... MUST be prepared for the possibility that this will result in unbounded recursion."	Duplicate	Other	Duplicate of issue #243
245	DoD	1 - Federal	General Line 2461	Interoperability continues to be a major challenge for Federal Agencies. DoD has a mission need to support interoperability with other Federal mission partners by exchanging attributes about individuals to assist in the account request/authorization, account provisioning, and account management processes within DoD IT assets. Currently, there are no specific federal solutions to support that activity. DoD plans to begin a production deployment of pilot Backend Attribute Exchange (BAE) implementation that mirrors the Federal ICAMSC BAE 2.0 documentation, but there are no other federal PIV issuers subscribers.	DoD recommends NIST codify the ICAMSC BAE 2.0 initiative for federal PIV issuers to share attributes. Each Federal PIV issuerer should be required to expose an Agency BAE broker so that other federal PIV issuers can exchange identity attributes and PIV records, where needed.	Declined	PIV Federation	Decline - This is out of scope of this publication.
246	DoD	1 - Federal	Appendix C Line 2656	There is no definition of Authenticator in Appendix and the concept is referenced in various places throughout the document (e.g., Sections 2.10.1 (Line 1108) and 3.1.2 (Line 1261)).	DoD recommends adding a definition of Authenticator to differentiate for the reader the difference between an authenticator and credential.	Accept	Derived PIV	Accept - Definition added to the glossary of FIPS201-3
247	NSA Center for Cybersecurity Standards	1 - Federal	2.9	This section is mostly silent on derived PIV credentials (2.9.4, lines 1085 and 1086 is the exception). If all derived PIV requirements are in 2.10, then there should be requirements that cover all of the Section 2.9 subsections.		Accept in Principle	Derived PIV	Accept in Principle - This is closely related to issue #248. Section 2.9.4 already addresses how Derived PIVs must be terminated when the PIV card is terminated. Per issue #248, the updated document text clarifies that non-PKI Derived PIVs do not need to be reissued when PIV cards are modified or reissues administratively.
248	NSA Center for Cybersecurity Standards	1 - Federal	2.9.1 and 2.10	Neither of these sections address the requirements for derived PIV credentials when the PIV is re-issued. The minimum would be to say that the original issuance method shall be followed.		Accept in Principle	Derived PIV	Accept in principle - Non-pki DPC (at least) will not require reissuance when the PIV is reissued. See also #234
249	NSA Center for Cybersecurity Standards	1 - Federal	2.9.1 Line 922	If the card has not been compromised, is collected and is destroyed, why is it necessary to revoke it (whatever it means to 'revoke' a card)? In addition, if the private keys have not been compromised, why is it necessary to revoke the keys on that card? [note: in the case of loss, stolen or compromised cards, I agree revocation is the only course]		Duplicate	PIV Card	Duplicate of issue #466

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
250	NSA Center for Cybersecurity Standards	1 - Federal	Section 3.1.1, lines 1238-1241	It seems so strange to see a card writer in a section called 'PIV Front-End Subsystem'. An end user is not classically using a card writer (printing/loading cards). Change 'card reader' to 'card reader/writer' in Figure 3-1. Change sentences 1 and 2 to: "Card writers may be used to perform remote PIV Card updates (see Section 2.9.2)."		Duplicate	PIV Card	Duplicate of issue #306
251	NSA Center for Cybersecurity Standards	1 - Federal	Section 4.2, line 1726	How is this asymmetric key set different than either the card authentication data or the PIV authentication data? Is there a use case that can't be handled by the 2 mandatory asymmetric key sets?		Declined	PIV Card	Decline - These are keys used for Secure Messaging, which uses a particular ECDH protocol.
252	NSA Center for Cybersecurity Standards	1 - Federal	Section 4.2.2, line 1798	Please define 'retired'. Or replace it with 'expired and revoked' (because sadly revocation is required when replacing these keys).		Accept	PIV Card	Accept- Now defined in Glossary
253	NSA Center for Cybersecurity Standards	1 - Federal	Section 5.5, lines 2125-2129	Requirements that dictate what needs to be in a certificate doesn't fit nicely into a section that discusses where CRLs and OCSP responders publish information. Consider moving it to Section 5.2.1, where the subject is 'X.509 Certificate Contents'.		Declined	Other	Decline - Section 5.5 covers certificate status information, which is the natural place to cover this material that is specific to CRLs and OCSP responders.
254	NSA Center for Cybersecurity Standards	1 - Federal	Section 5.5, lines 2130	This statement about Depts and agencies reporting at CA when certificates need to be revoked also doesn't fit nicely into this section. Consider moving this to Section 5.3, 'X.509 CRL Contents'.		Declined	Other	Decline - Section 5.3 is not a more appropriate section.
255	NSA Center for Cybersecurity Standards	1 - Federal	Appendix C	Appendix C, Card Management System: using the term in the definition is not normal. How about 'A system that manages the lifecycle of a PIV Card'?		Accept	Editorial	Accept
256	NSA Center for Cybersecurity Standards	1 - Federal	Appendix C	Appendix C, Card Verifiable Certificate: This is out of alphabetic order.		Accept	Editorial	Accept
257	NSA Center for Cybersecurity Standards	1 - Federal	Appendix C	Add a definition of 'certificate', and/or 'public key certificate'. Here is what is in CNSSI 4009: 'A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date).' It also has 'public key certificate' with a reference back to 'certificate'.		Accept	Editorial	Accept - Added definition of certificate (and italicize use in glossary pages).
258	Perspecta	2 - Industry	2.7.1 Line 780	"...issuer-controlled station, remote location, trained operator at a central location" - SP 800-63-3/2.4 allows for CSP's to be comprised of multiple independently-operated and owned business entities. Why should this not be extended to proofing? Should also align with language in 2.7.1 line 788.	The issuer may subscribe to or contract independently for trained operator services provided they are compliant with the NIST SP 800-63A specifications and guidance for SRIP.	Duplicate	Enrollment	Duplicate of issue #548

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
259	Pespecta	2 - Industry	2.7.1 Line 781	"..goal..is to permit identity proofing in remote locations where it is not practical for them to travel.."	Remote identity proofing allows for safe continued Identity Proofing operations (e.g., Social distancing)	Duplicate	Enrollment	Duplicate of issue #268
260	Perspecta	2 - Industry	2.7.1 Line 797	The introduction of draft statements requiring monitoring by staff at the station location are antithesis to the benefits and intent of SRIP	If the intent is security of persons/objects, the clarification must be made to differentiate from required proofing resources (i.e., trained operators).	Declined	Enrollment	Decline - see issue #580. However, note that additional clarifications will be addressed in SP 800-79.
261	Perspecta	2 - Industry	2.7.1 Line 796	The introduction of draft statements requiring monitoring by staff at the station location are antithesis to the benefits and intent of SRIP	Monitoring by staff can be adequately performed with the same level of security with mechanical / physical barriers and electronic (camera) means without staff phycially located at the station.	Duplicate	Enrollment	Duplicate of issue #580
262	NextgenID/STA	2 - Industry	See spreadsheet attached below, same error for several locations.	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	"Supervised Remote In-Person Proofing" or similar harmonized language should be used across all documents.	Duplicate	Enrollment	Duplicate of issue #515
263	NextgenID/STA	2 - Industry	2.7.1 Line 778	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	"Supervised Remote In-Person Proofing" or similar harmonized language should be used across all documents.	Duplicate	Enrollment	Duplicate of issue #515
264	NextgenID/STA	2 - Industry	2.7.1 Line 789	We suggest that section 2.7.1 of the FIPS 201-3 draft is both redundant and discordant in specifying operational parameters (e.g., see the precedent delineation of proofing requirements and guidance (i.e., local, remote, IALs, etc.) already defined in the Special Pubs Digital Identity Guidelines (NIST SP 800-63A, 800-63-3, et. al) thereby obviating the inclusion in FIPS 201-3)	The use of SRIP and requirements for SRIP SHALL adhere to the guidelines and requirements set forth in SP 800-63-3 and SP 800-63A for Supervised Remote _in-Person Proofing.	Duplicate	Enrollment	Duplicate of issue #545
265	NextgenID/STA	2- Industry	2.7.1 Line 795	SRIP is simply a special use case (remote operator v. local operator) of the already established IAL3 In-Person Identity Proofing as meticulously defined in SP 800 63-3 and SP 800-63A (5.3.3.2) Supervised Remote In-Person Proofing, wherein all informative and normative compliance specifications are detailed.	Supervised Remote In-Person Proofing SHALL meet the requirements and criteria in NIST SP 800-63A.	Duplicate	Enrollment	Duplicate of issue #546
266	NextgenID/STA	2 - Industry	2.7.1 Line 779	Process non-specific, implicit attribution to 800-63 is undefined	…MAY use the Supervised Remote In-Person Proofing process per the guidelines specified in NIST SP 800-63A for the issuance of PIV Cards. Suggest creating a highlevel section that combines items in Sect 2.7.1 line 779 - 819 and reference SP 800- 63 and 63A for specific details.	Duplicate	Enrollment	Duplicate of issue #547

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
267	NextgenID/STA	2 - Industry	2.7.1 Line 780	"...issuer-controlled station, remote location, trained operator at a central location" - SP 800-63-3/2.4 allows for CSP's to be componentized and comprised of multiple independently-operated and owned business entities. Why should this not be extended to proofing? Should also align with language in 2.7.1 line 788.	…a station in a controlled-access environment that is connected to a remote location for remote operation by a trained trusted-provider. The issuer may subscribe to or contract independently for trained operator services provided they are compliant with the NIST SP 800-63A specifications and guidance for SRIP. See comment on line 25	Duplicate	Enrollment	Duplicate of issue # 548
268	NextgenID/STA	2 - Industry	2.7.1 Line 781	"..goal..is to permit identity proofing in remote locations where it is not practical for them to travel.."	…Is to permit remote identity proofing at comparable levels of confidence and security to in-person events where it is not practical or safe (e.g., COVID) for them to travel to the agency for in-person identity proofing."	Declined	Enrollment	Decline - The suggested text as policy already exist to issue alternate credentials in case of COVID. Per [OPM policy memo](https://www.opm.gov/policy-data-oversight/covid-19/opm-memorandum-on-boarding-processes-for-new-employees-during-the-covid-19-emergency/), agencies are able to make risk-based decisions to issue alternative credentials in certain circumstances.
269	NextgeID/STA	2 - Industry	2.7.1 Line 786	should match verbiage from NIST SP 800-63A 5.3.3.2	…to achive comparable levels of confidence and security to in-person events." The draft attribution of "closely duplicate" is superfluous and erroneous as the use of SRIP technology can enhance and improve standard in-person proofing practices.	Duplicate	Enrollment	Duplicate of issue #550
270	NextgenID/STA	2 - Industry	2.7.1 Line 789	Obviated by delineated requirements specificed in NIST SP 800-63A 5.3.3.2	Contend that the draft content be deprecated as it should be further defined by NIST SP 800-63A 5.3.3 describing attributes exceeding the confidence and security attained by local operators/staff. Remove from FIPS 201-3.	Duplicate	Enrollment	Duplicate of issue #551
271	NextgenID/STA	2 - Industry	2.7.1 Line 797	SRIP is defined as Supervised Remote Proofing in Appendix A of NIST SP 800-63-3 as – A remote identity proofing process that employs physical, technical, and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. If the 800-63-3 definition holds than it is discordant with the draft FIPS 140-3 language “SHALL be monitored by staff at the station location…” and footnote 9 "...where staff can see the station while performing other duties."	Supervised Remote In-Person Proofing SHALL meet the requirements and criteria in NIST SP 800-63A.	Duplicate	Enrollment	Duplicate of issue #552
272	NextgenID/STA	2 - Industry	2.7.1 Line 797	The introduction of draft statements requiring monitoring by staff at the station location are antithesis to the benefits and intent of SRIP	If the intent is security of persons/objects, the clarification must be made to differentiate from required proofing resources (i.e., trained operators).	Duplicate	Enrollment	Duplicate of issue #260 and issue #533
273	NextgenID/STA	2 - Industry	2.7.1 Line 796, 797, footnote 9	The introduction of draft statements requiring monitoring by staff at the station location are antithesis to the benefits and intent of SRIP	What is meant by "monitored" and "staff" and for what purpose? Contend that the draft content be deprecated or further clarified as it is superceded by NIST SP 800-63A 5.3.3.2 describing attributes exceeding the confidence and security attained by local operators/staff.	Duplicate	Enrollment	Duplicate of issue #580

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
274	NextgenID/STA	2 - Industry	Line 796, 797, & footnote 9	Excludes requirements for physical security and integrity	Add "Shall employ physical tamper detection and resistance features appropriate for the environment in which it is located. " matching the requirements in SP 800-63A	Duplicate	Enrollment	Duplicate of issue #555
275	NextgenID/STA	2 - Industry	2.7.1 Line 798, 799	SRIP is to be completed in complete alignment with 800-63A specifications/practices for SRIP -by explicitly stating rules within FIPS-201-3, this runs high risk of diverging from the authority and preferred specification of 800-63A for SRIP.	Strike as not applicable. This level of specification is not needed at the superior document level.	Duplicate	Enrollment	Duplicate of issue #556
276	NextgenID/STA	2 - Industry	2.7.1 Line 796, 797, Footnote 9	Not required by 800-63A nor is it warranted as long as security and tamper detection is implemented	Strike as not applicable, Specification is not needed at the superior document level as full specification exists in 800-63A	Duplicate	Enrollment	Duplicate of issue #557
277	NextgenID/STA	2 - Industry	2.7.1 line 798, 799	Contrary to the notion of segmented enrollments	Language implies a single session. This is different from a segmented process. Need clarification of the language.	Duplicate	Enrollment	Duplicate of issue #558
278	NextgenID/STA	2 - Industry	2.7.1 Line 778-819	The language of proofing for a PIV identity is too restrictively focused on the issuer. The PIV program itself is built for federation, upon a common chain of trust for users issued PIV Identity. Proofing processes should not be considered an integral, mandatory role of the issuer. This role can optionally be fulfilled by a trusted 3rdparty	The language of proofing for a PIV identity is too restrictively focused on the issuer. The PIV program itself is built for federation, upon a common chain of trust for users issued PIV Identity. Proofing processes should not be considered an integral, mandatory role of the issuer. This role can optionally be fulfilled by a trusted 3rdparty See comment above.	Duplicate	Enrollment	Duplicate of issue #559
279	NextgenID/STA	2 - Industry	2.7.1 Footnote 9	Not required by 800-63A nor is it warranted as long as video surveillance, security and tamper detection is implemented	Strike as not applicable, Specification is not needed at the superior document level as full specification already exists in 800-63A Sec 5.3.3.1 and 5.3.3.2.	Duplicate	Enrollment	Duplicate of issue #580 and issue #550
280	NextgenID/STA	2 - Industry	2.7.1 Line 813-819	Include reference to 800-63A 5.3.3.1	"..per the criteria defined in [SP 800-76] and [SP 800-63A 5.3.3.1 and]..Sec 5.3.3.1 and 5.3.3.2.	Duplicate	Enrollment	Duplicate of issue #561
281	Dept. of Veteran Affairs	1 - Federal	2.4 Line 594, 595	Imaging from same fingers imaged for off-card one-to-one comparison represents a security vulnerability that can be used to unlock the card.	Replace SHOULD on line 594 with SHALL to make this a requirement rathen than a recommendation.	Duplicate	PIV Card	Duplicate of issue #512
282	Dept. of Veteran Affairs	1 - Federal	4.2.1 Line 1744 - 1778	NIST needs to specify when the CHUID authentication mechanism will no longer be an accepted practice so agencies can plan for this expensive an laborious transition of their PACS.	Provide an implementation timeline as well as provisions for the agency to identify and accept the inherent risk of non-compliance.	Duplicate	Authentication	Duplicate of issue #493.
283	Dept. of Veteran Affairs	1 - Federal	4.3.1 Line 2010 - 2012	Requiring the PIV card to compare the chosen PIN against commonly chosen values will warrant a card redesign, configuration changes to HSPD-12 systems, possibly slow down card performance and the deployment of a new card on the heels of the V8.1 card deployment. This change will require more work across the Federal enterprise than the expected benefits of the change.	Leave the selection of a secure PIN to agency policies and procedures at the time of card activation.	Duplicate	PIV Card	Duplicate of issue #589

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
284	Treasury	1 - Federal	2468	Since Federation SAML assertion does not specifically specify PIV or assurance level, how can a Replying Party ensure PIV-PKI authentication method was used by the user at the Identity Provider.	Identify a method so the Relying Party can ensure the proper assurance level (e.g., IAL1-3, AAL1-3 [PIV]) used meets their digital identity risk assesment requirements for that agency application.	Declined	PIV Federation	Decline - This is discussed explicitly in section 7.2.
285	Treasury	1 - Federal	2.4 Line 594	"With these updates, NIST is trying to clarify that the two fingerprints for off-card one-to-one comparison MAY be taken from the full set of fingerprints collected in Section 2.3 or collected independently. However, they left out the ""or collected independently"" phrase, which should be included for clarity. In addition, NIST is trying to clarify that the two fingerprints for OCC SHOULD be imaged from fingers not imaged for off-card one-to-one comparison. However, if this is actually a security risk, NIST should make this mandatory (SHALL). Note: USAccess does not currently support OCC."	The requirement to collect "Two fingerprints for on-card comparison (OCC). These fingerprints MAY be taken from the full set of fingerprints collected in Section 2.3 and SHOULD be imaged from fingers not imaged for off-card one-to-one comparison." should be clarified to remove any ambiguity. If there is a security concern with using the same two fingerprints imaged from fingers imaged for off-card one-to-one comparison as the two fingerprints for OCC, the word "SHOULD" should be replaced with "SHALL".	Duplicate	PIV Card	Duplicate of issue #512
286	Treasury	1 - Federal	4.2.1	"NIST added text to this section pertaining to the removal of the CHUID authentication mechanism and detailed the remaining purpose/use of the CHUID. They also added specifications for the Cardholder UUID and clarified that the content signing certificate SHALL NOT expire before the expiration of the card authentication certificate. NIST should specify the timeframe when the CHUID authentication mechanism must no longer be used or change this to allow Agencies to make a risk based decision about when to stop using it."	"NIST should specify the timeframe when the CHUID authentication mechanism must no longer be used or change this to allow Agencies to make a risk based decision about when to stop using it. This specific timeframe will allow for proper and systematic bugeting resulitng in greater compliance."	Duplicate	Authentication	Duplicate of issue #493.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
287	Treasury	1 - Federal	6.2.5	"NIST added the following requirements: (1) A maximum of 10 consecutive PIN retries SHALL be permitted unless a lower limit is imposed by the department or agency. (2) The PIN SHALL be a minimum of six digits in length. (3) The PIV Card SHALL compare the chosen PIN against a list of at least 10 commonly-chosen values (e.g., 000000, 123456) and require the choice of a different value if one of those is selected by the cardholder. We checked with the USAccess card vendor (Idemia) to determine if the v8.1 PIV Cards comply with these requirements, because otherwise a new card version will have to be developed/deployed. We were told that requirements 1 and 2 are supported, but not 3."	The new requirement for the PIV Card to "compare the chosen PIN against a list of at least 10 commonly-chosen values (e.g., 000000, 123456) and require the choice of a different value if one of those is selected by the cardholder" is not supported by the current USAccess PIV Cards. This would require the vendor to develop a new PIV Card version and issuers to replace these cards. In addition, we are concerned that this requirement would slow down the performance of the card without adding any significant level of security. Instead of this being added as a requirement, we think this should be a recommendation to the cardholders when selecting a PIN." There is little return on investment for this huge cost. Newly issue Cards should fall under this new requirement.	Duplicate	PIV Card	Duplicate of issue #589
288	Treasury	1 - Federal	6.2.5	"NIST removed the CHUID as an authentication mechanism in this version of the Standard. The CHUID data element itself, however, has not been removed and continues to be mandatory as it supports other PIV authentication mechanisms. NIST should specify the timeframe when the CHUID authentication mechanism must no longer be used or change this to allow Agencies to make a risk based decision about when to stop using it."	"See row above The new requirement for the PIV Card to ""compare the chosen PIN against a list of at least 10 commonly-chosen values (e.g., 000000, 123456) and require the choice of a different value if one of those is selected by the cardholder"" is not supported by the current USAccess PIV Cards. This would require the vendor to develop a new PIV Card version and issuers to replace these cards. In addition, we are concerned that this requirement would slow down the performance of the card without adding any significant level of security. Instead of this being added as a requirement, we think this should be a recommendation to the cardholders when selecting a PIN."""	Duplicate	Authentication	Duplicate of issue #493 NOTE: the comment refers to removal of CHUID. The suggested change by the commenter recommends change to the PIN requirements.
289	Department of Energy	1 - Federal	293	Section 2.4: Biometric Data Collection for PIV card states that "Two fingerprints for On Card Comparison …MAY be taken from full set of fingerprints… and SHOULD be imaged from fingers not imaged for off-card one-to-one comparison."	For PIV card security purposes, "Two fingerprints for On Card Comparison …MAY be taken from full set of fingerprints… and SHALL be imaged from fingers not imaged for off-card one-to-one comparison."	Duplicate	PIV Card	Duplicate of issue #512
290	Department of Energy	1 - Federal	1745	Section 4.2.1 requires that the CHUID (Card Holder Unique Identifier) no longer be used for physical access card authentication.	Given the size and expense of complying with this requirement, NIST must either publish a timeline for implementing and give agencies time to allocate funds or allow agencies to make risk-based decisions about when they will comply.	Duplicate	Authentication	Duplicate of issue #493

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
291	Department of Energy	1 - Federal	1997	Section 4.3.1 limits the number of failed attempts at establishing a PIN during card activation to 10. Also requires enforcement of mechanisms to prevent the applicant from selecting unsecure PINs.	Per HSPD-12 vendor (Idemia), this would require a new PIV card creation and deployment. Current measures for secure PIN creation and could possibly slow down card performance. Recommend agencies enforce this as a process when cardholder is selecting a PIN.	Declined	PIV Card	Decline - The requirement limits the number of failed attempts to unlock a a card to use the PIV Auth key, and perform other functions that require the card to be unlocked. It does not refer to the number of attempts to initially set the PIN.
292	Health and Human Services (HHS)	1 - Federal	4.3.1 Line 2010 - 2012	"The reference as written suggests the PIV Card edge will enforce this new mandatory feature for PIV Activation, as well as PIN resets. This new requirement will make existing card stock incompatible once the Standard and dependent NIST Special Publications become effective. HHS requests guidance added for adequate transition timelines to deplete the existing inventory of previously purchased products, time for new products to become available, and for PIV systems to be updated. Rationale: There are multiple technological solutions that make up the ability to create, update and use PIN numbers for PIV credentials (e.g., the PIV card, Middleware, and Card Issuance Systems). We believe some agencies maintain PIN data differently, such as requiring a PIN change immediately after personalization to prevent Card Management System (CMS) from having record of the initial PIN. Additionally, many agencies have purchased APL PIV card stock in bulk as agencies plan months and years ahead for their expected volume of card holders. "	"Return of implementation schedule guidance 10. Implementation Schedule. This Standard mandates the implementation of new PIV Card features. To comply with FIPS 201-3, 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 or of the depending new or revised NIST Special Publications. Accreditations of PIV Card issuers (PCIs) that occur 12 months after the effective date of this Standard shall be in compliance with FIPS 201-3."	Duplicate	Other	Duplicate of issue #339

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
293	Health and Human Services (HHS)	1 - Federal	6.2.5 Line 2342 - 2343	"Request to keep CHUID as a deprecated feature for layered access control implementations. This would allow agencies to design cost effective implementations that require PKI authentication at the perimeter access points but allow persons to move between areas with equal or less interior security requirements utilizing existing readers and relying infrastructure. Rationale: Many agencies, HHS included, still heavily rely on CHUID for PACS authentication in their facilities. An overhaul of PACS readers and the CHUID technology is a massive overtaking, requiring funding approval from agency leadership, effective and efficient project management, and the ability to balance this project with other key initiatives."	The CHUID authentication mechanism is no longer allowed under FIPS-201 as an authenticator for entry into secured access control points. As the CHUID authentication mechanism provides LITTLE or NO assurance in the identity of the cardholder, CHUID MAY only be used after successful authentication at the perimeter of a layered access control system to allow persons to move between interior areas having equal or less security requirements. It is expected that this limited use of the CHUID authentication mechanism will be removed from this Standard at the next five-year revision. Agencies SHALL plan a full transition away from CHUID as an authentication method across their facilities.	Duplicate	Authentication	Duplicate of issue #215
294	Health and Human Services (HHS)	1 - Federal	2.7.1 Line 779 - 819	"HHS requests language that codifies that Supervised Remote Identity Proofing stations may be used for the issuance of credentials (both PIV and Derived) in addition to identity proofing, registration and PIV Card Activation Reset. Rationale: With the controls required by this draft to complete remote identity proofing, we believe there should be allowances for remote issuance processes as well, as long as they follow similar, if not more stringent controls. Agencies would require FIPS guidance on how to properly perform these actions. Additionally, in the current operating environment we face due to COVID-19 - we believe we should entertain all possibilities in order to assist remote user populations, and high-risk applicants across the government."	"Departments and agencies MAY use a supervised remote identity proofing station for the processes involved in the issuance of PIV Cards and Derived PIV credentials. This involves the use of an issuer-controlled station at a remote location that is connected to a trained operator at a central location. The goal of this arrangement is to permit identity proofing of individuals in remote locations where it is not practical for them to travel to the agency for in-person identity proofing and issuance of their PIV credential."" The issuer SHALL have local trained staff to perform card custodian operations such as receiving and controlling centrally printed card stock when the station is used for the issuance of PIV Cards. C.1 Glossary of Terms Card Custodian An individual who has been trained to support local Supervised Remote Identity Proofing processes and can monitor the station during operations, securely control card stock received from the central location, and generally assist users during the identity	Accept in Principle	Enrollment	Accept in Principle - A new section was added to specify that supervised remote idenity proofing station can support PIV card issuance.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
295	SSA	1 - Federal	2.4 Line 600 - 604	For individuals who have a reciprocal background investigation on file, it would not be possible to perform a biometric match against original 10 prints. Reciprocity means that some individuals do not need to be re-fingerprinted to send fingerprints to the FBI as recent favorable investigation occurred and is on file They agency may not have access to the fingerprints since none are collected due to reciprocity, they may not be the originating agency who requested the on file investigation.	Add additional language to clarify this is not required for reciprocity cases.	Accept in Principle	Enrollment	Accept in Principle - See rationale #364 on same/similar subject.
296	SSA	1 - Federal	6.2.5 Line 2342 - 2343	"CHUID Authentication, while insecure, is the only authentication mechanism with proven technologies in the market. CAK-based solutions require industry maturity and few SM-AUTH-based solutions are on the market. Additionally it is unclear whether SM-AUTH solutions have gone through the FICAM Test Lab or per comment on A.5 have operational viablity. SM-AUTH may be immature solutions that may be expensive and degrade physical security operations. Removing the CHUID authentication mechanism due to insecurity, creates additional risks for agencies as there is no clear replacement that doesn't also introduce a wide variety of challenges to overcome given industry immaturity. "	Acknowledge that there is not an equivalent replacement for CHUID authentication and that the market is required to mature to meet newer authentication standards. Clarify if SM-AUTH solutions completed FICAM Test Lab validation.	Declined	Authentication	Decline - CHUID authentication was deprecated in the previous revision. No extension is warranted.
297	SSA	1 - Federal	6.3.1 Table 6-1	"1.) SYM-CAK has been deprecated and is included in the table 2.) SM-AUTH should be added to the table"	Remove SYM-CAK, Add SM-AUTH	Accept in Principle	Editorial	Accept in Principle - The document text was updated to add (deprecated) text to SYM-CAK (it's allowed in the table even though deprecated) - Table 6.1 has been revised by adding SM-AUTH
298	SSA	1 - Federal	A.5 Line 2581 - 2588	The FIPS 201 Validation program including the FICAM test lab should not be the only program that establishes whether products conform since these programs do not validate comprehensive operational viability nor accreditation of SP800-53 controls as a requirement.	Expand the validation program to include feedback from the federal community.	Declined	Other	Decline - While we agree in principle, what is being described is out of scope for the FIPS 201 Evaluation Program.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
300	N/A	4	4.2.2.1 PIV Authentication Key (1836-1839), 4.2.4 PIV Unique Identifiers (1971-1989), 6.2.3.1 Authentication with the PIV Authentication Certificate Credential (PKI-AUTH) (2272-2274), 7.3 Benefits of Federation (2504-2506)	Interoperability and federation between different federal departments and agencies require PIV cardholder identitifiers that are unique within the PIV (and PIV-I) identity management space. This is a long-standing mission need and gap also related to implementing FPKI and PIV-I (Federal and Non-Federal Issuers) logical access control using the PIV Authentication certificate and implementing identity provider (IdP) services such as the Backend Attribute Exchange Broker demonstrated by DHS and DoD.	Mandate that the last 16 digits of the Federal Agency Smart Card Number (FASCN) uniquely identify the cardholder for the Executive branch and other federal partners (congress, courts, state, local, territory, tribe, etc.) conform with existing ISO, NIST FIPS/SP attributes for PIV, PIV-I, PIV-C, etc., and its location as a cardholder identifier field for both the card and PIV authentication certificate. The DoD and VA construction of the PIV Authentication certificate Subject Alternative Name will include an Other Name:Principal Name field constructed by concatenating the last 16 digits of the FASCN with "@federal agency abbreviation" (e.g., last 16 digits of FACSN@mil or last 16 digits of FASCN@va). DMDC and VA intend to use this construction to aid with interoperability and onboarding new federal entities to the Federal Electronic Health Record system.	Duplicate	Other	Duplicate of issue #239
301	N/A	4	4.2.4. PIV Unique Identifiers	The VA is adopting the DoD's Electronic Health Record system which currently uses the DoD EDI-PI as the unique identifier. The current plan is to provision EDI-PIs to all VA personnel (~730K) requiring access to the joint system, as well as VA patients (~9million) that far outnumber the DoD patient population. This is not a sustainable solution as it makes VA dependent on DoD to provision and manage identity attributes of VA personnel and patients. Had there been a federally unique identifier, this situation would not have occurred. A more sustainable solution for such situations is to embed a federally unique identifier on the PIV card itself that allows for an ecosystem of identity providers to perform delegated authentication and authorization services without the need for creating new "unique" identifiers.	Include language in the FIPS 201-3 that mandates using the last 16 digits of the Federal Agency Smart Card Number (FASCN) to uniquely identify the cardholder for the Executive branch and other federal partners. The DoD and VA construction of the PIV Authentication certificate Subject Alternative Name will include an Other Name:Principal Name field constructed by concatenating the last 16 digits of the FASCN with "@federal agency abbreviation" (e.g., last 16 digits of FACSN@mil or last 16 digits of FASCN@va). DMDC and VA can then use this construction to aid with interoperability and onboarding new federal entities to the Federal Electronic Health Record system.	Duplicate	Other	Duplicate of issue #239

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
304	Rick Uhrig	4 - Self	2.9.4 Line 1071	The phrase "Similar to the situation in which the PIV Card is compromised, normal termination procedures must be in place" suggests that the topic of PIV Card termination subsequent to card compromise has previously been addressed. This is misleading.	Replace with "PIV Card termination procedures must be in place for both normal circumstances as well as suspected card compromise"	Declined	Other	Decline - The proposed text appears to conflate termination (where eligibility for a PIV card is lost) and revocation for lost/stolen cards. Revocation is covered in Section 2.9.1.
305	Rick Uhrig	4 - Self	Line 901, 903, 928, 934, 988, 1071	The term "compromised" is used 6 time in FIPS 201-3 with regard to the PIV Card or one of its logical credentials, without ever explicitly stating what qualifies as a card or logical credential being compromised	Explicitly state the conditions that require and individual or agency to consider that a card or logical credential has been compromised.	Declined	Other	Decline - Agencies/issuers should use their own discretion to determine conditions sufficient to deem a card compromised.
306	Rick Uhrig	4 - Self	3.1.1 Line 1238	"The sentence ""Card writers, which are similar to card readers, personalize and initialize the information stored on PIV Cards."" is completely misleading. Three reasons: 1. For smart card technology, the ISO/IEC standard name for this equipment is ""Card Accepting Device"". These are commonly (and informally) called ""Card Readers."" They are never called ""Card Writers."" 2. All the reading and writing is done by the card's chip itself, based on commands (and perhaps authorizations and authentication) received from the Card Accepting Device. 3. There is no difference whatsoever in card accepting devices that perform read operations vs. those that perform write operations. They merely pass the command on to the chip."	Find a way to lose the term "Card Writer." E.g., replace the sentence with "'Card Accepting Devices', commonly called 'card readers', transmit commands to PIV Cards for either reading data from, or writing data to, PIV Cards. Card readers are also used to personalize and initialize the information stored on PIV Cards"	Declined	Other	Decline - The term "card writer" is used as part of the functional description of the component in the PIV front-end subsystem.
307	Rick Uhrig	4 - Self	3.1.2 Line 1268	The phrase "from generation and loading of authentication keys and PKI credentials" is unnecessarily narrow. The exact same can be said for digital signing and key management keys. What they have in common is that they are all asymmetric private/public key pairs. (Also, if restricted to just authentication keys. the "and loading" piece does not apply.)	Replace with "from generation and loading of asymmetric keys and PKI credentials"	Accept	Editorial	Accept
308	Rick Uhrig	4 - Self	4.1.4.1 Line 1530	Table 4-1 is not complete and cannot be reviewed		Duplicate	PIV Card	Duplicate of issue #218 part 4
309	Rick Uhrig	4 - Self	4.1.4.3 Line 1630-1632	The phrase "red SHALL be reserved for emergency response offcials, blue for foreign nationals, and green for contractors." has two implied SHALLs Consider rewording to remove the implied SHALLs	Replace with "the following color coding SHALL be used: red for emergency response officials, blue for foreign nationals, and green for contractors."	Accept	Editorial	Accept

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
310	Rick Uhrig	4 - Self	4.1.5 Line 1700	Figures 4-3, 4-4 and 4-4 all show cards with an expiration date that is 6 years + 1 day after the issue date, giving the card an apparent validity period of 6 years and 2 days. These appear to be examples of correctly formatted cards with invalid validity periods.	For Figures 4-3, 4-4, and 4-5, change either the issue date or expiration date of each example so that the PIV Card validity period is <= 6 years	Accept in Principle	Editorial	Accept in Principle - Dates on examples have been revised.
311	Rick Uhrig	4 - Self	4.2.2.1 to 4.2.2.7	There is a subtle difference between the "SHALL" and "SHALL only" constructs that seems to be overlooked in these sections. E.g., in 4.2.2.2, the phrase "SHALL be available through the contact and contactless interfaces of the PIV Card." requires that the capability be present on each of the two stated interfaces. In contrast, in 4.2.2.5, the phrase "SHALL only be accessible using the contact and virtual contact interfaces of the PIV Card." requires only that capability not be accessible on any other interface. It is completely silent as to whether the capability must be accessible on the contact or virtual contact interfaces. This seems contrary to the actual intent.	"Although tedious, it is perhaps best to specific, complete and consistent for all these subsections. e.g. ""If this key is present, cryptographic operations using the PIV Card's digital signature key SHALL be available through the contact interface, SHALL be available through the virtual contact interface, and SHALL NOT be available through the contactless interface."" Be consistent with the use of ""available"", ""accessible"", or ""performed"". Choose one. Be consistent with the use of ""through"" or ""on."" Choose one. Section-specific recommendations follow."	Partially Accept	Editorial	Partial Accept - Changes to Section 4.2.2.1-4.2.2.7 clarified the cryptographic operations and keys that can be used over the contact, contactless, and virtual contact interfaces. As part of these changes, we avoided "shall only" constructs to improve clarity and readability.
312	Rick Uhrig	4 - Self	4.2.2.1 Line 1832-1833	"The cryptographic operations that use the PIV authentication key SHALL be available only through the contact and virtual contact interfaces of the PIV Card." unnecessarily separates "SHALL" and "only". Also, it does not require that the operations be available on either of the named interfaces.	Replace with "The cryptographic operations that use the PIV Card's authentication key SHALL be available through the contact interface, SHALL be available through the virtual contact interface, and SHALL NOT be available through the contactless interface."	Accept in Principle	PIV Card	Accept in Principle - Changes to Section 4.2.2.1-4.2.2.7 clarified the cryptographic operations and keys that can be used over the contact, contactless, and virtual contact interfaces. As part of these changes, we avoided "shall only" constructs to improve clarity and readability.
313	Rick Uhrig	4 - Self	4.2.2.2 Line 1852 - 1853	"The statement ""Cryptographic operations that use the card authentication key SHALL be available through the contact and contactless interfaces of the PIV Card."" is silent on the virtual contact interface"	Replace with "Cryptographic operations that use the asymmetric card authentication key SHALL be available through the contact, virtual contact, and contactless interfaces of the PIV Card."	Declined	PIV Card	Decline - The proposed text would result in text saying a required feature would need to be available over an optional interface. The existing text does not prohibit the CAK from being used over VCI.
314	Rick Uhrig	4 - Self	4.2.2.3 Line 1874 - 1875	The statement "The cryptographic operations that use the card authentication key SHALL be available through the contact and contactless interfaces of the PIV Card." is silent on the virtual contact interface.	Replace with "If this key is present, cryptographic operations that use the symmetric card authentication key SHALL be available through the contact, virtual contact, and contactless interfaces of the PIV Card."	Declined	PIV Card	Decline - The proposed text would result in text saying a feature would need to be available over an optional interface. The existing text does not prohibit the (now deprecated) symmetric card authentication key from being used over VCI.
315	Rick Uhrig	4 - Self	4.2.2.4 Line 1879-1881	"If this key is present, cryptographic operations using the digital signature key SHALL be performed using the contact and virtual contact interfaces of the PIV Card." does not require the key to be available on the contact or virtual contact interfaces. This does not seem to be the intent.	Replace with "If this key is present, cryptographic operations using the PIV Card's digital signature key SHALL be available through the contact interface, SHALL be available through the virtual contact interface, and SHALL NOT be available through the contactless interface."	Accept in Principle	PIV Card	Accept in Principle - The updated text clearly defines what operations SHALL or SHALL NOT be available through a contact or contactless interface.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
316	Rick Uhrig	4 - Self	4.2.2.5 Line 1890-1892	"If present, the cryptographic operations that use the key management key SHALL only be accessible using the contact and virtual contact interfaces of the PIV Card." does not require the key to be available on the contact or virtual contact interfaces. This does not seem to be the intent.	Replace with "If this key is present, the cryptographic operations that use the PIV Card's key management key SHALL be available through the contact interface, SHALL be available through the virtual contact interface, and SHALL NOT be available on the contactless interface."	Accept in Principle	PIV Card	Accept in Principle - The updated text clearly defines what operations SHALL or SHALL NOT be available through a contact or contactless interface.
317	Rick Uhrig	4 - Self	4.2.2.6 Line 1900-1901	"If present, the cryptographic operations that use the PIV Card application administration key SHALL only be accessible using the contact interface of the PIV Card."	Replace with "If present, the cryptographic operations that use the PIV Card application administration key SHALL be available through the contact interface, SHALL NOT be available through the virtual contact interface, and SHALL NOT be available on the contactless interface.""	Accept in Principle	PIV Card	Accept in Principle - The updated text clearly defines what operations SHALL or SHALL NOT be available through a contact or contactless interface.
318	Rick Uhrig	4 - Self	4.2.2.7 Line 1905-1907	"The cryptographic operations that use the PIV secure messaging key SHALL be available through the contact and contactless interfaces of the PIV Card."	Replace with "If present, the cryptographic operations that use the PIV secure messaging key SHALL be available through the contact, virtual contact, and contactless interfaces of the PIV Card."	Declined	PIV Card	Decline - There are no situations where the secure messaging keys themselves would be used over VCI (as opposed to being used over the contactless interface to establish the VCI). Therefore, the existing text is appropriate.
319	Yubico	2 - Industry	2.10 Line 217	Given the existance of modern hardware-backed security technolgy, the PIV card needs to be modernized via innovation.	Existing PIV cards should be paired with a strong, secure, modern authenticator as the minimum new standard. Support strong access on any endpoints with standard derived credentials that are available in new form factors that don't require traditional dedicated readers. This structure should leverage APIs, incorporate modern strong authentication capabilities such as FIDO, and provide management tools to support per agency use and enterprise device management.	Noted	Other	Noted - While we're not incorporating the specific text change, the underlying concepts will be reflected in the broader set of work on Derived PIV Credentials during the FIPS 201-3 revision cycle.
320	Yubico	2 - Industry	4.2 Line 235	"The PIV Card provides multiple capabilities in one form factor: Logical Access to IT systems, physical Access for building access, flash pass badge as an identity document. While this convergence of the multiple capabilities provides a single authenticator, it does not lend itself to reduced complexity in a number of scenarios. "	Allowing derived credentials on additional authentication form factors that are purpose-built for streamlined strong authentication, such as security keys, allows for strong authentication without having to strictly conform to the physical PIV card form factor.	Noted	Derived PIV	Noted - Line number reference in the comment points to incorrect line(235) Section 4.2 starts at line 1701. Authentication methods described in section 6.3 have updated and clarified; that DPC can be different form factors.
321	Yubico	2 - Industry	2.1 Line 217	Expand the definition of derived credential	A modern hardware-based, single purpose security device is a sound approach that provides agencies and their users the option to store derived credentials in one place and to use them on many different computing devices. Benefits include reduced costs and complexity. In addition, the credential can be stored on an inexpensive Government Furnished Equipment (GFE) like a security key. This enables the BYOD use case and ensures the credential is stored securely on the GFE.	Noted	Derived PIV	Noted - FIPS 201-3 expands the notion of derived credentials to other form factors and to non-PKI authenticators. Updates to SP 800-157 will provide more details. The COMMENT Should reference section 2.1 beginning at line 506.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
322	Yubico	2 - Industry	2.7 Line 704	Allow for a single Identity Proofing event to produce multiple credentials which can be held on different authentication devices (such as a PIV card and a Security Key).	This enables maximum efficiency and security. Align Identity Proofing with IAL3 summarized in 800-63-3A to allow supervised remote presence. Further, when issuing derived credentials to new authenticators , allow existing credentials issued with strong (IAL3) identity proofing to be used as proof of identity.	Noted	Enrollment	Noted - This is closely related to the concept of derived credentials described in issue #321
323	Yubico	2 - Industry	2.7 Line 207	Modern authentication technologies allow for secure remote issuance.	Technologies such as manufacturer Attestation Certificates and Secure Channel Protocol 03 (SCP03) can ensure that the Security Key presented is a known and trusted credential. Modern Security Keys support this secure remote issuance for both the PIV and FIDO credentials.	Noted	Enrollment	Noted - Such technologies will be considered for Derived PIV Credentials in the revision to SP 800-157.
324	Yubico	2 - Industry	7.2 Line 272	Start with the fact that Federation Assurance Level 3 is good for high security, but hard to implement. Tap industry to find the solution.	Strong hardware-based direct authentication is preferable to Federation. New technologies, such as FIDO WebAuthn or cloud services, such as Microsoft Azure, can be utilized in place of Federation without necessitating additional friction in the user experience. Federation flows should not just limit strong authentication on initial login but based on risk levels, perform 2nd factor authentication or re-authentication against the PIV credential.	Noted	PIV Federation	Noted - The intend in FIPS201-3 is to define model that uses Federation with PIV cards.
325	Yubico	2 - Industry	N/A	See attached spreadsheet	See attached spreadsheet [fips201-3-Yubico_Additional_Comments_Without_Sec._&_Line_info..xlsx](https://github.com/usnistgov/FIPS201/files/5945880/fips201-3-Yubico_Additional_Comments_Without_Sec._._Line_info.xlsx)	Noted	Other	Noted - These are general comments that did not seek specific changes in FIPS 201-3.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
326	XTec, Inc.	2 - Industry	4.2.2.3 / 6.2.4 Line 1865 / 2316	"FIPS 201-3 should NOT deprecate either the SYM-CAK key or the SYM-CAK authentication mechanism. There are 3 reasons: 1. SYM-CAK, used in combination with PKI-CAK (“Plan A/Plan B”), offers Federal Departments and Agencies greater benefits than PKI-CAK used alone. 2. Deprecating SYM-CAK will stifle agency use and vendor innovation, to the disadvantage of Federal Departments and Agencies 3. NIST’s published criteria for “deprecated and removed features” do not justify deprecating SYM-CAK. A separate document has been submitted on GitHub with detailed explanations for each of these reasons for NOT deprecating SYM-CAK."	"DO NOT deprecate the SYM-CAK key or the SYM-CAK authentication mechanism."	Duplicate	PIV Card	Duplicate of issue #207
327	XTec., Inc	2 - Industry	4.3.1 Line 2008	"Guessable/Identifiable PINs: The draft states ""The PIN should not be easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number or phone number). "" This is written in the passive voice, obscuring how the control is enforced (i.e. by the informed cardholder), and that issuers have a responsibility to provide guidance as part of cardholder training."	Change the statement to the active voice. “The cardholder SHOULD NOT choose a PIN that is easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number or phone number).”	Duplicate	PIV Card	Duplicate of issue #589
328	XTec., Inc	2 - Industry	4.3.1 Line 2010	"PIN Checking on PIV Card: The draft states ""The PIV Card SHALL compare the chosen PIN against a list of at least 10 commonly-chosen values (e.g., 000000, 123456) and require the choice of a different value if one of those is selected by the cardholder."" XTec understands that card manufacturers find this requirement problematic to implement on the card."	Delete the requirement for this to be enforced by the PIV Card. If desired, add "The cardholder SHOULD avoid commonly chosen values"	Duplicate	PIV Card	Duplicate of issue #589

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
329	XTec., Inc	2 - Industry	4.3.1 Line 2010	"PIN Checking on the CMS/Middleware: The draft states ""The PIV Card SHALL compare the chosen PIN against a list of at least 10 commonly-chosen values (e.g., 000000, 123456) and require the choice of a different value if one of those is selected by the cardholder."" There has been discussion within industry that this control could be enforced elsewhere, such as in middleware or within the issuer's card management system. However, such an implementation would allow the control to be circumvented easily. Anytime after post issuance, a cardholder could merely change the PIN using an alternate capabaility that does not enforce the control, e.g. the default Windows 10 PIN change feature allows unrestricted PIN changes (other than PIN-length enforcement by the PIV card). To see how this is easily accomplished, we refer you to: https://pivkey.zendesk.com/hc/en-us/articles/204375395-How-do-I-change-the-user-PIN- . PIN-changes can also be accomplished using other available online tools and middleware. This control can ONLY be consistently and effectively implemented by the card, and not by any	"DO NOT change this requirement so that some other component of the system (e.g. the middleware or CMS) is responsible for implementing the control to check against a list of commonly-chosen values. Delete the requirement. It is not practicle to implement on the PIV Card nor within the CMS/middleware."	Duplicate	PIV Card	Duplicate of issue #589

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
330	XTec., Inc	2 - Industry	2.10.1 Line 1111-1113	"Derived Credential Binding to PIV Account: The draft states “Derived PIV credentials SHALL be bound to the cardholder’s PIV account only by the organization that manages that PIV account.” The language seems to imply that Derived PIV credentials can only be issued by the PIV issuing organization. This would be contrary to SP800-157. As organizations look to leverage already issued PIV credentials and as more applications enable Derived PIV authentication many use cases that support federation and interoperability arise. Specifically, an organization’s desire to leverage the PIV identity proofing already performed and issue a Derived PIV for temporary/limited application use for their organization. For example, FEMA has detailees that support disasters and come from various agencies. FEMA issues these federal employees smart phones to support the mission. If a detailee is from GSA, FEMA should be able to leverage their GSA PIV card to issue a FEMA derived certificate to the FEMA device the GSA detailee is using. "	"1. Remove sentence because it conflicts with SP800-157. Alternately, clarify that a PIV Card Issuer and a Derived Issuer to do not have to be the same entity which is consistent with SP 800-157 and SP 800-63. Clarify that binding is not issuance. 2. Clarify that an “Organization” is not necessarily a “PIV Card Issuer”. Reference 800-157 language whereby there is guidance for separate issuing organizations in Section 2.4: “A Derived PIV Credential issuer shall only issue a Derived PIV Credential to an Applicant if it has access to information about the Applicant’s PIV Card from the issuer of the PIV Card. […] Additional methods must be employed for obtaining information about the PIV Card from the PIV Card issuer”. "	Declined	Derived PIV	Decline - This was discussed at length during the FIPS 201-3 drafting process. In order to keep the status of Derived PIVs aligned with the status of the PIV card and the attributes in the PIV Account, Derived PIVs must be managed by the PIV Issuer. This requirement does not prohibit organizations from issuing other (non-PIV) credentials based on possession of PIV.
331	XTec, Inc.	2 - Industry	General	"Relying Party", "Relying System" and "Relying Subsystem": These terms are used for what appears to be the same thing.	"1. If these terms are refering to the same entity, it is suggested that a single term be used throughout FIPS 201-3 for consistency and to avoid confusion. Note that SP 800-63-3/63A/63B/63C use the term ""relying party"". 2. If these terms are meant to refer to different entities, add each term to ""Appendix C.1 Glossary of Terms"" so that any distinctions between each is clarified."	Accept in Principle	Editorial	Accept in Principle - Document updates define "Relying System" and "Relying Subsystem" as the same term, will use "Relying Party" and "RP" in only federation contexts.
332	XTec., Inc	2 - Industry	General	Other Types of Issued Derived PIV Credential Digital Certificates: Agencies may deliver Digital Signing Certificate, Encryption Certificates and Encryption Key History Keys along with Derived Credential Authentication Certificates for derived credentials issued to mobile device.	Review and address these additional certificates and keys where they may apply in the draft standard. Also, take into consideration for the next version of SP 800-157.	Declined	Derived PIV	Decline - This is out of scope for FIPS201. Digital Signature, and encryption keys (both current and historic) are not authentication credentials in the way the PIV Card's authentication credentials or derived PIV credentials are. Digital Signature and encryption keys are used for a different purpose and thus DPC requirements do not apply. Nevertheless, both digital signature and encryption certificates are covered in SP 800-157 and will continue to be covered (updated) in the new version of SP 800-157.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
333	XTec., Inc	2 - Industry	2.2 Line 568	"Continuous Vetting Program: Section 2.2 (Credentialing Requirements) states ""Once the investigation is completed, the authorized adjudicative entity SHALL adjudicate the investigation and report the final eligibility determination to the Central Verification System (or successor). This determination SHALL be recorded in the PIV enrollment record to reflect PIV eligibility for the PIV cardholder and, if applicable, their enrollment in the Continuous Vetting Program."" Continuous Vetting Program is only mentioned once in the draft and not defined. "	Define "Continous Vetting Program" within FIPS 201-3, expanding on its impact/significance to Credentialing Requirements and any other relevant requirements. Also, add this term to "Appendix C.1 Glossary of Terms"	Accept in Principle	Enrollment	Accept in Principle - We have refreferenced Executive Order 13764 which provides a good definition of Continuous Vettiing > 'Continuous vetting' means reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements.
334	XTec., Inc	2 - Industry	2.7	"Temporary Resident Card: Temporary Resident Card has been removed from the list of Forms of Identification. Was this intentional? Was this document replaced by another?"	Verify that this change/deletion was intentional.	Noted	Enrollment	Noted - I-688 (temporary resident card) has been removed because it was retired by DHS and subsequently removed as an I-9 listed id document.
335	DHS	1 - Federal	Line 82-97	"6.1 Special-Risk Security Provision Does this now mean an agency like DHS should look for PIV card vendors that support a high-assurance on/off switch for the contactless interface? In so doing, may these cards now be used in high-side applications?"	"If turning off ""wireless"" or the contactless interface is now required depending on deployment risk, this must be formally defined. Most likely in §2. Otherwise, PIV card vendors may not add the capability. Formally define that biometrics are now optional. If high risk facilities are to be recognized and biometrics are not to be placed on the card to mitigate risk, this must be specified precisely, enabling issuers NOT to place fingerprint templates, facial images, or OCC fingerprints on the card. Otherwise, not including fingerprint templates is a non-compliant card and will not pass 800-79 audit."	Declined	PIV Card	Decline - This section is a description of exceptions to the requirements in the document, not making requirements optional for all cards.
336	DHS	1 - Federal	Line 95-97	Could use of the physical PIV Smart Card be mitigated by other form factors and be applicable here? Recommend adding language enabling derived PIV credentials as mitigation mechanisms. Example given may be Fido. This needs an industry discussion with card manufacturers and CMS vendors.	Suggest: "Use of other risk-mitigating methods such as alternate credentials (e.g., Derived PIV, Fido), or technical means within the PIV card (e.g., high-assurance on/off switches for the wireless capability), or procedural mechanisms in such situations is preferable and, as such, is also explicitly permitted and encouraged."	Declined	Derived PIV	Decline - While other authenticators like FIDO are likely non-PKI derived PIV credentials, it's not clear what risks they would mitigate that are associated with the PIV Card.
337	DHS	1 = Federal	Line 135-137	Will SP800-73 now specify the secure wireless switch for high security applications ensuring NPIVP will test for that security feature?	See comment on lines 82-97. FIPS 201-3 must explicitly define the contactless switch and no fingerprints/facial over contactless.	Duplicate	PIV Card	Duplicate of #335

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
338	DHS	1 - Federal	Line147-144	None of the specifications listed here ensure that an E-PACS lock properly interoperates with a PIV card for security and interoperability. The ICAMSC PIV in E-PACS provides those controls.	Incorporate ICAMSC PIV in E-PACS as an authoritative document. Or formally establish it within SP800-53. Strengthen the APL's role to enforce these controls.	Noted	PIV Card	Noted - This is out of scope for FIPS 201-3, but we will cover this issue in the next revision of SP 800-116.
339	DHS	1 - Federal	Line 147-151	9 Effective Date This statement does not take into consideration product development cycles, issuance lifecycle, nor relying party application lifecycle. It does not provide effective leadership for the infrastructure of the PIV system.	Recommend something like the following: 1. NIST must update SP800 series (i.e. -73, -76, -78, -79, -157) and related within six months of FIPS 201-3 release. 2. Products (e.g., PIV cards, CMSs) must comply with mandatory features within 1 year of SP800-73 series update (largely due to long certification cycles). 3. Issuers shall initiate issuance of compliant PIV cards (mandatory features) as soon as Products are available. 4. Relying party systems shall be updated with mandatory features within six months of issuer test cards being available.	Accept in Principle	Other	Accept in Principle - Effective date language has been updated to reflect current guidance.
340	DHS	1 - Federal	Line 165-174	11 Qualifications This is true enough. The standard can not dictate how to build the relying party systems. But in the case of E-PACS, there are no governing standards on how to build those systems (unlike the plethora of LACS standards).	Incorporate ICAMSC/ISC PIV in E-PACS as an authoritative document. Or formally establish it within SP800-53. Or make PIV in ICAMSC/ISC E-PACS a NIST SP800-xx document. See comment to 147-151 on timelines. Strengthen the APL's role to enforce these controls.	Duplicate	Other	Duplicate of issue #338
341	DHS	1 - Federal	Line 365-367	"…in the use of PIV accounts."	Should be: "…in the use of Identity account." "accounts" is a relying party application term and not applicable to PIV in this context.	Declined	Other	Decline - PIV Account terminology will be updated to define PIV Identity Account.
342	DHS	1 - Federal	Line 417-422	"new PIV Cards SHOULD NOT" - this is not a statement of requirement - more of an opinion, not a normative statement.	Revise sentence beginning with However - However, deprecated features shall not be incorporated into new PIV card stock.	Declined	PIV Card	Decline - Will change language to "card stock" where appropriate
343	DHS	1 - Federal	Line 448-462	This is a long list of special publications that impact the success of the PIV system. Is there a coherent release schedule of updates to these publications to aid in product development, issuance, and relying party applications?	Update the special publications in a fully coordinated way to aid in product development, issuance, and relying party systems deployment. See comment to lines 147-151.	Noted	Other	Noted - Will pass on suggestion to teams updating Special Publications.
344	DHS	1 - Federal	Line 540-542	2.1 Control Objectives This now states that "...expired … credentials are swiftly revoked."	Expired credentials are not serviceable after expiration. This should state "…invalidated credentials are swiftly revoked." removing the OR condition that adds expired. Requiring revocation of expired credentials bloats CRLs unnecessarily. Define what "invalidate" means in the definitions, and provide the "shall" use cases, the "should" use cases, and the "do not" use cases for revocation / invalidation.	Accept in Principle	Other	Accept in Principle - Updated document text clearly states that a process exists to invalidate, revoke, or destroy credentials when the cardholder loses eligibility or when the credential is lost, stolen, or compromised.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
345	DHS	1 - Federal	Line 566-568	"This determination SHALL be recorded in the PIV enrollment record to reflect PIV eligibility for the PIV cardholder and, if applicable, their enrollment in the Continuous Vetting Program." There is no concept of an enrollment record that is authoritative for an individual's identity. The enrollment record is just that. An enrollment record. The Enterprise IDMS is authoritative for adjudication of enrollment data and the status of an identity within an agency. New hires are not already enrolled and must be enrolled for the first time for continuous vetting.	Should be "This determination SHALL be recorded in the Enterprise Identity Management System to reflect PIV eligibility for the individual and, if applicable, their enrollment or re-enrollment in the Continuous Vetting Program."	Declined	Enrollment	Decline - PIV enrollment record is intended to be a broader term than the record in the Enterprise IDMS. Also, see how this section is rephrased in Issue #227
346	DHS	1 -Federal	Line 587-588	"2.3 Biometric Data Collection for Background Investigations : ""These fingerprints MAY be taken from the full set of fingerprints collected in Section 2.3.""""	"""…MAY…"" should be ""…SHALL…"" to effectively maintain the chain of trust between background investigation and credentialing. An exception should be allowed where ""Two fingerprints for off-card one-to-one comparison may be collected only after 1:1 biometric comparison of the applicant with the fingerprints collected in Section 2.3."" This too maintains the chain of trust. Recommend allowing authentication via priority order of authentication in SP800-76, based off of the original two biometrics set for authentication (i.e., primary and secondary). Authentication shall always take place, before changes can be made to biometric and biographic (e.g., name) information, via a system enforcement methodology. "	Declined	Enrollment	Decline - You may copy the fingerprints from those taken for the background investigation, but you don't need to. But we require chaining to address the risk that is being alluded to here.
347	DHS	1 - Federal	Line 587-589	"2.3 Biometric Data Collection for Background Investigations ""These fingerprints MAY be taken from the full set of fingerprints collected in Section 2.3...""""	"""…MAY…"" should be ""…SHALL…"" to effectively maintain the chain of trust between background investigation and credentialing. An exception should be allowed where ""Two fingerprints for OCC may be collected only after 1:1 biometric comparison of the applicant with the fingerprints collected in Section 2.3."" This too maintains the chain of trust."	Duplicate	Enrollment	Duplicate of issue #346.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
348	DHS	1 - Federal	Line 618-620	"OCC MAY be used to support card activation as described in Section 4.3.1. OCC MAY also be used for cardholder authentication (OCC-AUTH) as described in Section 6.2.2."	These statements appear limiting in nature to cardholder authentication events. Recommend OCC also be authorized for PIV issuance and maintenance processes (as are the Off-Card Comparison Fingerprints and Iris).	Accept in Principle	Authentication	Accept in Principle - Updates to the document text clarified when OCC MAY be used in a normative context.
349	DHS	1 - Federal	Line 629-633	"The image MAY be used for cardholder authentication (BIO or BIO-A) as described in Section 6.2.1."	This should make automated facial recognition for cardholder authentication legitimate. Both at time of issuance and for card lifecycle maintenance.	Noted	Authentication	Noted - Updates to document in Section 2.5 allow this.
350	DHS	1 - Federal	Line 632-633	"""...authentication during operator-attended PIV issuance and maintenance processes…"""	Instead of operator-attended, why not specify BIO-A as required? Is this actually a statement that Facial for BIO is insufficient when compared to fingerprint or iris?	Declined	Enrollment	Decline - However, requirements will be rephrased per issue #514
351	DHS	1 - Federal	Line 635-639	"...the applicant SHALL be linked through a positive biometric verification decision by comparing biometric characteristics captured at a previous session with biometric characteristics captured during the current session."	in this fashion? Recommend requiring 1:1 biometric authentication against the original enrollment 10-print for all sessions until issuance is complete. This strengthens chain-of-trust.	Declined	Enrollment	Declined - This would be a new requirement imposed on department and agencies. FIPS 201-2 was not that stringent - nor does it need to be since biometric matching against previous biometrics collected achieves the same goal. It does not have to be against the 10-print in all cases.
352	DHS	1 - Federal	Line 642	should use The instead of A to designate a specific group.	"The card issuer"	Accept	Editorial	Accept
353	DHS	1 - Federal	Line 646	"...cardholder's PIV account."	This should be "…individual's identity account within the Enterprise IDMS." It truly is not a "PIV account," as the identity account may receive a PIV, CIV, PIV-I, Derived PIV. These are benefits of having the identity account and being vetted for an appropriate credential (the benefit) based on need.	Duplicate	Other	Duplicate of issue #341
354	DHS	1 - Federal	Line 650-670	"PIV enrollment records SHOULD include the following data: ….." How can federated interoperability take place, if there are not a minimum set of ""shall"" requirements in the enrollment record?	Recommend breaking the sub-bullets up into "shall" statements, AND "should" statements. Determined the required data set needed for a base level "enrollment record" for all agencies to achieve, in order to trust the credential issued. The "should" statements would be ones to achieve before the next release of FIPS 201 (i.e., 201-4).	Duplicate	Other	Duplicate of issue #368

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
355	Electronic Privacy Information Center (EPIC)	3 - Academia	See attachment	See attachment	See attachment [EPIC-NIST-PIV-FIPS-Feb-2021-Comments.pdf](https://github.com/usnistgov/FIPS201/files/5946787/EPIC-NIST-PIV-FIPS-Feb-2021-Comments.pdf)	Partially Accept	Other	Parrtially Accept - 1) The commenter requested anonymous credentials suitable for direct, offline authentication. FIPS 201 specifies a suite of credentials, including PKI credentials supporting direct, offline authentication without intermediaries. Device or anonymous authentication mechanisms would not support important use cases that require fine-grained access control or auditing. While there may be unidentified use cases within the Federal enterprise that could benefit from such privacy-enhancing technologies, the lack of industry-supported standards and products would make such a major architectural change to federal identity management impractical at this time. NIST will continue to consider technical, procedural and policy privacy controls as we develop additional standards and guidelines for PIV, including privacy protection of identity attributes as we develop guidelines on the use of federation. 2) limit all collection and use of biometric data to 1:1 matching with a biometric profile encoded on the identity card, not stored in a virtual database //The biometrics used for authentication are stored on-card to enhance privacy. This removes the need for central database access during authentication. Note: Other forms of biometric collection is within the context and constraints of federal laws, regulations, and policies. For example, collection of fingerprints is part of the federal hiring process as per OPM (e.g. federal employment and PIV eligibility determination).
356	DHS	1 - Federal	Line 652	"...and what data was collected."	Recommend: Recommend this be codified explicitly in SP 800-156.	duplicate	Other	Duplicate of issue #368
357	CertiPath Inc.	2 - Industry	General	All imperatives utilize SHALL whereas recent guidance has indicated use of this word is discouraged in favor of MUST. Not saying I necessarily agree, just pointing it out. https://www.plainlanguage.gov/guidelines/conversational/shall-and-must/	Replace SHALL with an alternate imperative, for example MUST	Declined	Editorial	Decline - We define our normative language in the appendix.
358	DHS	1 - Federal	Line 662	"The record MAY contain historical unique identifiers."	"This should be ""The record MAY the contain the Cardholder UUID and historical unique identifiers."" The Cardholder UUID is an important new artifact, as it pairs with the PI value, as does the Card UUID with the FASC-N Identifier, both found within the FASC-N. The Cardholder UUID should be renamed to Person UUID, as it never changes over time and should not be confused with CHUID."	Accept in Principle	Editorial	Accept in Principle - Will add language to suggest inclusion of Cardholder UUID in PIV Enrollment Record.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
359	CertiPath Inc.	2 - Industry	2.1 Line 520-522	"A proper authority authorizing issuance happens before the identity vetting process. Suggest ""appropriately vetted"" deserves some explanation. This is the first time it is used and it doesn't appear in the glossary."	Reorder the sentence as follows: A credential is issued to an individual only after a proper authority has authorized issuance of the credential, the individual's identity has been verified, and the individual has been appropriately vetted.	Accept in Principle	Enrollment	Accept in Principle - Document text was re-worded to: A credential is issued to an individual only after a proper authority has authorized issuance of the credential, the individual's identity has been verified, and the individual has been vetted per section 2.2.
360	CertiPath Inc.	2 - Industry	2.1 Line 523-529	The use of the word 'eligibility' seems out of place here. Eligibility for a credential depends on things like being a federal employee or contractor. The background investigation speaks to suitability. An individual may be eligible but not suitable.	Replace 'eligibility' with 'suitability' here and in other appropriate locations.	Declined	Enrollment	Decline - "Eligibility" is the correct term, as covering both "suitability" and "fitness."
361	DHS	1 - Federal	Line 669-670		"This should be ""...the issuer SHALL include the evidence of a formal name change."" Without evidence, the chain-of-trust for the identity record is broken. Changing to SHALL is consistent with §2.7 lines 723-724."	Accept in Principle	Other	Accept in Principle - Per issue #368, we did not intend to specify normative requirements for data elements in the PIV enrollment records. The use of "SHOULD" in this bullet is thus potentially confusing, and it will be revised accordingly.
362	CertiPath Inc.	2 - Industry	2.2 Line 557-559	Flow would be improved if this paragraph preceded the paragraph above (beginning on line 550)	Move paragraph.	Declined	Editorial	Declined - Second paragraph contains the main point, third is additional.
363	CertiPath Inc.	2 - Industry	2.2 Line 560-563	This sentence is awkward	"Reword as follows: For individuals for whom no prior investigation exists, the appropriate required investigation MUST be initiated with the authorized federal investigative service provider and the FBI NCHC portion of the background investigation MUST be completed and favorably adjudicated prior to PIV Card issuance."	Accept in Principle	Editorial	Accept in Principle - Sentence was re-worded as follows: "For individuals for whom no prior investigation exists, the appropriate required investigation SHALL be initiated with the authorized federal investigative service provider and the FBI NCHC portion of the background investigation SHALL be completed and favorably adjudicated prior to PIV Card issuance."
364	CertiPath Inc.	2 - Industry	2.3 Line 580-582	This statement runs afoul of subsequent statements that require comparison of two fingers to 10 fingers throughout certificate life cycle. (See lines 600-604 and footnote 6 for example). This should state that the 10 fingerprints must be retrievable from this prior clearance. There is also later reference to the investigation not being more than 12 years old which is not captured here.	Revise this paragraph to accurately reflect later requirements, particularly the need to retrieve the 10 prints from the original documentation and that the investigation can't be more than 12 years old.	Accept in Principle	Enrollment	Accept in Principle - Introduction paragraph was added at top of section 2.3. See also #295 and prior resolution wrt re-connecting to 10 print in case where there is an adjudication on record (It is not the intent to re-connect in this case per DoD-11 resolution from FIPS 201-2 comment resolution. The 12 year refers to biometrics to be stored on-card and stored in enrollment record. There is no statement on investigation expiration date. OPM guidelines apply in this case.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
365	CertiPath Inc.	2 - Industry	2.4 Line 587-588	"Should there be an 'if applicable' here? 2.3 references not collecting fingerprints in a Tier 1 or higher investigation is on record. This could suggest it is appropriate to pull these fingerprints from that older record. In later sections there is reference to 'no usable prints' but perhaps that should be discussed here. From personal experience, I know that people with perfectly good fingers are sometimes physically unable to provide usable templates."	"Revise this bullet to add ""if applicable"" or some other language that clarifies the two print collection. Consider adding some discussion here of the unavailability of usable prints even when the actual fingers are present and accounted for."	Declined	Enrollment	Decline - The text being commented on says that you **may** take them from the fingerprints taken for the background investigation. Other sections expand on the requirements for biometric data.
366	DHS	1 - Federal	Line 672	"...maximum of 12 years."	suggest defining what a year is as being 365 days or in the case of 12 years 365 days plus applicable days for leap years. This may need to be specified explicitly in SP 800-79 and should be added to SP 800-76. This also affects long term certificates within FPKI Common Policy.	Declined	Editorial	Decline - A few days isn't going to materially affect this time limit enough for us to have an internal definition.
367	CertiPath Inc.	2 - Industry	2.4 Line 596-599	Is this limited to electronic biometric verification attempts? Back to the fingerprint issue. If usable fingerprints cannot be collected, is a visual comparison of facial image acceptable.	Clarify the meaning of "biometric verification attempt"	Accept	Enrollment	Accept - Updated text clarifies "biometric verification attempt".
368	CertiPath Inc.	2 - Industry	2.6 Line 645	Why does this state "are generally". Isn't PIV account interoperability across agencies enhanced by mandating the minimum data set that must be collected and maintained?	Consider revising this paragraph to indicate the id proofing, registration and biometric enrollment artifacts must be maintained as part of the cardholder's PIV account.	Declined	Other	Decline - This issue was considered during previous FIPS 201 revision cycles. Individuals agencies and issuers can determine what data elements are maintained in the PIV enrollment records.
369	DHS	1 - Federal	Line 671-672	"The biometric data records in the PIV enrollment records SHALL be valid for a maximum of 12 years…."	"This should state ""The biometric data records in the PIV enrollment records and on PIV cards SHALL be valid for a maximum of 12 years."" As written, it is not clear that operational use of biometrics on a PIV card can not use bio that is older than 12 years."	Declined	Other	Decline - The 12-year timeframe on biometric data on the PIV card is covered in Section 2.9.1.
370	CertiPath Inc.	2 - Industry	2.7 Line 729	The F of foreign is lower case, even though the rest of the bullets start with a capital letter	Capitalize the F of foreign	Declined	Editorial	Decline - Other bullets start with proper nouns (except for drivers license, which is also lowercase.
371	CertiPath Inc.	2 - Industry	2.9.1 Line 909	Use of the term "adjudicative entity" - this term is not defined in the glossary.	Provide some context/definition for the term adjudicative entity.	duplicate	Enrollment	Duplicate of issue #388
372	DHS	1 - Federal	Line 690-695	"A PIV cardholder loses their card." Although reissuance is described further down in the document, a reader could read this and think that reissuance only applies to a lost PIV credential.	"Recommend new language be: ""Reissuance has multiple use cases; for example, a PIV cardholder loses their card."" "	Accept in Principle	Enrollment	Accept in Principle - Updated text emphasizes this is merely an example. e.g., "A PIV cardholder, for example, loses their card."
373	CertiPath Inc.	2 - Industry	2.9.3 Line 993-994	"A maximum of 10 consecutive PIN retries SHALL be permitted unless a lower limit is stipulated by the department or agency." should be two sentences.	Revise to state: "A maximum of 10 consecutive PIN retries is permitted. Individual departments and agencies may stipulate lower maximum retry limits."	Accept in Principle	Editorial	Accept in Principle - Updated text states "No more than 10 consecutive PIN retries SHALL be permitted. Card issuers MAY further restrict the maximum retry limit to a lower value."

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
374	DHS	1 - Federal	Line 696-703	A federal employee is . While it is technically possible to transfer an enrollment package / processed identity - there are no processes in place today to support enrollment exchange between issuers.	Update sentence to refer to mutual auth secure channel with receipt so it can be defined in 800-156.	Accept in Principle	Other	Accept in Principle - FIPS 201-3 generalized the concept of Chain-of-Trust to include all types of PIV enrollment records. In doing so, we may have lost some of the context around the original purpose of Chain-of-Trust, which was, in part, to facilitate transfer of enrollment records from one agency to another. Updates in Section 2.6 of document clarify how PIV enrollment records are handled.
375	DHS	1 - Federal	Line 705-707	"Identity proofing and registration requirements for the issuance of PIV Cards meet Identity Assurance Level (IAL) 3 since they follow a tailored process based on [SP 800-63A] IAL3 requirements."	"It is generally understood that IAL3 requires verification of ID documents against the original issuer. For the ""tailored process,"" is this required? Verification against the issuer, especially considering the state of driver's licensing across the states and territories, means that it may not be technically feasible. DHS recommends either clarify the requirement, or not require verification against the issuer. Is the language in lines 760-764 be sufficient to cover this requirement? That is because ""....a federal background investigation is considered a compensating control for identity proofing at IAL3.""?"	Accept in Principle	Enrollment	Accept in Principle - A note was added to describe how compensating controls (in the form of federal background investigations) are used to achieve IAL3.
376	DHS	1 - Federal	Line 731	"...driver's license or ID card that is compliant with [REAL-ID]…"	will be difficult. Per DHS press release on 2020-01-24, "The states now report to DHS that they have collectively issued more than 95 million REAL ID-compliant driver's licenses and ID cards (34%) out of 276 million total cards." REAL ID is not at 80% deployment yet and may effectively remove the ability to use a driver's license as form of ID for PIV enrollment.	Accept in Principle	Enrollment	Accept in Principle - Updates to document text clarify that the intent is to require Real ID in alignment with DHS's timeline for requiring Real ID.
377	DHS	1 - Federal	Line 796-797	"The station SHALL be maintained in a controlled-access environment and SHALL be monitored by staff at the station location while it is being used."	This bullet should be struck and operational deployment issues should be identified in SP 800-79. This may include privacy barriers, as well as deployment in controlled access areas. SP 800-63A already requires tamper resistance and the scene camera to protect the act of enrollment. Adding staff to monitor the enrollment does not improve the security of the enrollment based on SP 800-63A requirements.	Duplicate	Enrollment	Duplicate of issue #580
378	CertiPath Inc.	2 - Industry	3.1 Line 1206	In addition to physical and logical access, cards and credentials can be used for signature and key management, should that be mentioned here?	Consider adding signature and confidentiality to the reasons the cardholder uses the card in this introductory statement	Declined	Other	Decline - Other sections of FIPS 201 address this topic.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
379	DHS	1 - Federal	Line796-797	"...SHALL be monitored by staff at the station location while it is being used.9"	"This requires double the personnel to use SRIP, essentially defeating the purpose of the centralized Enrollment Official. In the DHS context, an intent was to field SRIP stations within the airport environment, or in DHS facility hallways, which are unlikely to have staff or E-PACS video available to monitor the station. Recommend adding requirements to further define ""monitored by staff."" Could the Issuer put agreements in place with GSA and other agencies who provide security guard staff at entrance points to federally controlled facilities, who could meet this requirement? Could the Issuer put agreements in place with the E-PACS that has video monitoring for the station? These agreements extend the audit boundary for enrollment and may not be sustainable."	Duplicate	Enrollment	Duplicate of issue #580
380	CertiPath Inc.	2 - Industry	3.1 Figure 3.1	Certificate Authority should be Certification Authority	Replace Certificate with Certification	Accept	Editorial	Accept - "Certification Authority" is used within the document elsewhere (and is in the glossary).
381	CertiPath Inc.	2 - Industry	3.1.1 Line 1223	In other locations future tense has been replaced with present tense. Should that be the case here?	Replace "will be" with "is"	Accept	Editorial	Accept
382	DHS	1 - Federal	Line 811-812	"...a mutually authenticated protected channel."	"...a mutually authenticated protected channel using FIPS approved encryption algorithms."	Noted	Enrollment	Noted - FIPS 201 already includes a general requirement to use FIPS validated cryptography.
383	CertiPath Inc.	2 - Industry	Line 1225	"might"?	Replace "might" with "may"	Declined	Editorial	Deline - "may" sounds too close to a normative MAY.
384	CertiPath Inc.	2 - Industry	Line 1230-1232	"Alternatively" suggests DPIV credentials can replace PIV cards.	"Reword as follows: ""Additionally, derived PIV credentials play an increasingly important role as authenticators, especially in environments where use of the PIV Card is not easily supported.""""	Accept	Derived PIV	Accept
385	CertiPath Inc.	2 - Industry	3.3 Line 1342-1350	Why is the federation protocol "recommended". Use of the strongest credentials on a PIV card do not require federation. This is Federal organizations accepting PIV for access, which means the need for 'assertions' about identity is largely moot. While there is certainly value to a federation approach, there are also drawbacks (single point of failure, MITM attack). Use of the term recommended has the potential to be misinterpreted.	Remove the 'recommendation' language here and talk about direct and federation in equal terms.	Declined	PIV Federation	Decline - "recommended" is the intended direction and strength.
386	CertiPath Inc.	2 - Industry	4.1.4.1 Table 4.1	It does not appear that examples (note none are included) would fit well into the table's third column. As it stands, this is not as helpful as the original table.	"Remove the third column and show how the name would be displayed on the card in the first (Name) column. Strange artifact in the footer should be removed."	Duplicate	Editorial	Duplicate of issue #218 (part 5)

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
387	CertiPath Inc.	2 - Industry	4.1.4.3 Line 1595	Here and in other locations: If deprecated, there should be some advice about ceasing or limiting use. As it stands now, it sounds like deprecated doesn't have any particular expectations for behavior associated with it. This coupled with statements like "it may be removed from future versions" doesn't convey the notion that organizations should move away or limit use.	Revise language throughout where a practice or item is being deprecated to explain what actions agencies should be taking regarding use of the deprecated practice or item. Alternatively, include some language in the introductory section concerning deprecated practices/items that can be referenced.	Declined	Other	Decline - Deprecated does not mean disallowed, nor does it necessarily mean there is a security issue.
388	DHS	1 - Federal	Line 825 and throughout	"PIV Cards SHALL be issued only after the adjudicative entity…." "Adjudicative entity"" is not defined. "	Recommend "adjudicative entity" be defined, and to also go a step further and associate the term "Registrar" with this (e.g., personnel security entities, etc.)	Accept	Enrollment	Accept - Add definition of "Adjudicative Entity." Decline to add "Registrar", per issue #428
389	DHS	1 - Federal	Line 835-838	"Before the PIV Card is provided to the applicant, the issuer SHALL perform a one-to-one comparison of the applicant against biometric data records available on the PIV Card or in the PIV enrollment record." As the language stands, it would seem that it is okay to perform a one-to-one biometric authentication after the card is printed and activated, but before an issuer hands the card (or ships the card) to an individual.	Recommend that the language be updated to explicitly require that a one-to-one authentication SHALL occur before a PIV Card is issued and activated, to ensure it is the same identity being issued to, before any changes occur to the card or identity record.	Declined	Enrollment	Decline - The suggestion would invalidate current implementation and there are safeguards in place (will be provided ONLY after successful biometric comparison). See also #399.
390	DHS	1 - Federal	Line 842-845	"If the biometric verification decision is negative, or if no biometric data records are available, the cardholder SHALL provide two identity source documents (as specified in Section 2.7), and an attending operator SHALL inspect these and compare the cardholder with the photograph printed on the PIV Card."	In the modern era of document forgeries, this may no longer be sufficient. Humans do not do a good job of facial recognition. Recommend the same IAL3 process against documents listed in §2.7 to improve the reliability of this decision to release the PIV card to the applicant.	Declined	Enrollment	Decline - A fallback option is needed if biometric verification fails. NIST is encouraging automated facial recognition algorithms by considering them a form of a biometric comparison.
391	DHS	1 - Federal	Line 864-868	"...and thus incur a short employment lapse period,…"	"There are a lot of scenarios or examples, but recommend listing the grace period for a Federal Contractor who becomes a Federal Employee (or vice versa). Fairly common, and their may be a gap of employment. Recommend that a timeframe be given. At some point in time, large employment lapses are no longer acceptable. ""Short"" needs to defined. Each agency background investigation entity (adjudicative entity? Registrar?) may have different requirements for this, making interoperability difficult. Recommend a timeframe be added in for all to follow at a minimum (i.e., six months). "	Declined	Enrollment	Decline - Draft FIPS 201-2 had 60 days in its public commenting draft. We received comments on FIPS2-1-2 from others indicating that OPM does not specify a time period and to please remove a specific time period. As a result, we removed the time. [comments](https://csrc.nist.gov/CSRC/media/Publications/fips/201/2/final/documents/fips201_2_2011_draft_comments_and_dispositions.pdf) (DHS-3 and DoD-20) See also footnote 12. where more context is given wrt lapse of time'

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
392	DHS	1 - Federal	Line 880-885	"If the biometric verification decision is negative, or if no biometric data records are available, the cardholder SHALL provide two identity source documents (as specified in Section 2.7), and an attending operator SHALL inspect these and compare the cardholder with the electronic facial image retrieved from the enrollment data record and the photograph printed on the new PIV Card."	§2.7 requirements, those of 842-845, and here, should line up. Recommend ID document verification in accord with SP800-63A IAL3, not just specifying the document types to use.	Partially Accept	Enrollment	Partially accept - Document will be updated to indicate that automated algorithmic facial recognition will be considered a biometric match. Facial image data may not be on the PIV card to support OCC but the information may be available in PIV enrollment records.
393	DHS	1 - Federal	Line 902-903	"The cardholder may also apply for reissuance of a PIV Card if one or more logical credentials have been compromised."	The prior sentence states "...a PIV Card that has been compromised…". This includes compromise of a "logical credential" such as the PIN that activates a PIV-AUTH credential. This sentence is a duplicate. Recommend deleting it. Any compromise forces re-issuance.	Declined	Enrollment	Decline - We want to be explicit that you may reissue the card if the logical credentials have been compromised. We think it is clearer to keep both, although we acknowledge the point the commenter made.
394	DHS	1 - Federal	Line 907-909	"If the expiration date of the new PIV Card is later than the expiration date of the old card, or if any data about the cardholder is being changed, the card issuer SHALL ensure that an adjudicative entity has authorized the issuance of the new PIV Card."	"Essentially, any time you re-issue a card, by definition, its expiration date will be later than the prior card. Recommend clarifying this. Tier 1 is a 5 year decision. What is really the desired outcome here? Confirm the individual is still PIV eligible in the identity record? Does the Tier 1 or Continuous Evaluation force re-adjudication updates within the identity record? Does the re-issued card have a shorter expiration date?"	Declined	Enrollment	Decline- Eligibility needs to be verified by the adjudicative entity, which could be an automated process.
395	DHS	1 - Federal	Line 913-914	"The issuer SHALL perform a biometric verification…"	" E.g., card nearing expiration and re-issuance occurs. What modalities?"	Accept	Enrollment	Accept - Updated document text clarifies that OCC is allowed.
396	DHS	1 - Federal	Line 917-921	…inspect documents…	See comment for 880-885	Duplicate	Enrollment	Duplicate of issue #392 (except that comment applies to a different line number).
397	DHS	1 - Federal	Line 950-952	"Key management keys and certificates MAY…"	"This has dual meaning. KMK may be generated/certified by CA and injected onto the card. That is fine. You could also read this is KMK may not be required when DigSig is required. Please clarify."	Accept	Enrollment	Accept - Updated document text clarifies that for cardholders who are required to have a digital certificate and key management certificate, they shall be generated or re-imported (in the case of the KMK).
398	DHS	1 - Federal	Line 989-990	The title of the section relates to "activation reset," yet the language starts out by discussing "PIN" on a PIV Card "may need to be reset."	Recommend the title of the section be updated to "PIV Card PIN Reset for Activation."	Duplicate	Editorial	Duplicate of Issue #218 (part 1)

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
399	DHS	1 - Federal	Line 999-1000	"...before providing the reset PIV Card back to the cardholder..."	"What happens if you reset the PIN and the biometric match fails? Recommend reducing risk. Recommend new language ""…before resetting the PIV Card's PIN…"" You really should know who is sitting with you prior to enabling the card for operational use again. Recommended change is consistent with 1016-1018."	Declined	Other	Decline - The suggestion would invalidate current implementation and there are safeguards in place (will be provided ONLY after successful match)
400	DHS	1 - Federal	Line 942	"...no later than 12 years…"	See comment to line 672.	Declined	Other	Decline - Studies show that biometrics remain matchable for >12 years, which aligns with PIV card lifecycles.
401	DHS	1 - Federal	Line 1001-1003	"...positive biometric verification decision when compared to biometric data records stored either on the PIV Card or in the PIV enrollment record."	"Is OCC allowed here? What modalities/authentication modes are allowed here?"	Accept	Other	Accept - Updated document text clarifies that OCC is allowed.
402	DHS	1 - Federal	Line 1003-1009	…inspect documents…	See comment for 880-885 Maybe use OCC language in 1014-1015.	Duplicate	Enrollment	Duplicate of issue #392 (except that comment applies to a different line number).
403	DHS	1 - Federal	Line 1025-1029	Is OCC allowed here?	What modalities? Vendors support both fingerprint and iris for on-card-comparison.	Duplicate	Enrollment	Duplicate of issue #584. We clarified that Biometric comparison can be done against data on the PIV card or in PIV enrollment records.
404	DHS	1 - Federal	Line 1040-1041	"The operator authenticates the owner of the PIV Card through an independent procedure."	What does this mean? Should this not be a statement consistent with IAL3? Is this a reference to the Global Platform PIN Unblock Key?	Duplicate	Enrollment	Duplicate of issue #218, sub-bullet 2
405	DHS	1 - Federal	Line 1053-1056	…inspect documents…	See comment for 880-885	Duplicate	Enrollment	Duplicate of issue #392 (except that comment applies to a different line number).
406	DHS	1 - Federal	Line 1075	CVS or successor shall be updated to reflect the change in status. What role does CVS or any successor play in PIV issuance?	There is no mention of CVS (or successor) prior to this bullet. CVS's role is not understood. Recommend a discussion with OPM occur to determine what role CVS would/could play? Determine if this is about adjudication status or issuance status.	Accept in Principle	Enrollment	Accept in Principle - Document text is updated to reflect latest OPM guidance on reporting eligibility status to CVS and to support enrollment into Continuous Vetting Program
407	DHS	1 - Federal	Line 1087-1088	This timeline should be in sync with PKI CRL lifetimes of the Agency	"If the card cannot be collected, normal termination procedures SHALL be completed within the CRL validity period of the Agencies PIV issuance CA." This is to account for not all agencies use 18 hours as the CRL validity period. DHS uses 24 hours.	Declined	PIV Card	Decline - Normal termination procedures are more than report/issue CRL (see line 1074-1092) - including removing FASC-N from any databases, which should be possible to do within 18 hours. CRL issuance is covered in section 5.3 line 2108 and it does state to follow COMMON for issuance of CRL.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
408	DHS	1 - Federal	Line 1108-1110	"The issuer SHALL attempt to promptly notify the cardholder of the binding of a derived PIV credential through an independent means that would not afford an attacker an opportunity to erase the notification."	It is not clear what risk is being mitigated by this statement. The focus of the sentence is notification of binding, yet the binding happens with positive participation of the recipient by using their PIV card. It may be that "…the binding of a derived PIV credential…" is actually ""binding and issuance"". In that context, positive affirmation of the receipt of the issued derived PIV credential is important. Clarify.	Declined	Derived PIV	Declined - The extra round-trip of providing a positive conformation doesn't add substantially to security and interferes with usability.
409	DHS	1 - Federal	Line 1111-1113	"Derived PIV credentials SHALL be bound to the cardholder's PIV account only by the organization that manages that PIV account."	Update "account" to be "identity account."	Accept in Principle	Derived PIV	Accept in Principle - Document text has been updated to rephrase term as "PIV identity account" to clarify.
410	DHS	1 - Federal		"Derived PIV credentials SHALL be bound to the cardholder's PIV account only by the organization that manages that PIV account."	"1. There may be a need for a detailee from one agency to receive a Derived PIV from another agency (e.g., DoD detailed to DHS) when they receive a managed mobile device from the detailed assignment agency (DHS). As written, if I am detailed from one agency to another, if I need a Derived PIV in the new agency, the new agency must issue a second PIV to the detailee. Is that the desired affect here? For those striving for one identity/one PIV, this may not work well. Should this restriction apply only to the managed mobile device receiving a credential being managed by the same agency that issued the derived PIV? 2. Concur, clarification is needed. Is the intent to trust the PIV issued from an outside agency (e.g., detailee coming from DOJ to DHS), and be able to issue a derived PIV off of the original issued PIV? Or, is the requirement for the agency being detailed to, will issue a second PIV card (e.g., have a DOJ PIV and a DHS PIV) and then bind the derived credential to the detailed agency PIV? "	Duplicate	Derived PIV	Duplicate of issue #330
411	DHS	1 - Federal	Line 1115 and throughout	"Derived PIV credentials SHALL be invalidated in any….."	Define "invalidated" in the glossary.	Accept	Derived PIV	Accept - This term is used several times in FIPS 201.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
412	DHS	1 - Federal	Line 1124-1125	"...contains a derived PIV authentication certificate..."	Concerns of invalidation/revocation must be expanded to include all derived PIV credentials. Derived PIV Authentication is just one of them. Derived should expand to all future use cases, such as Fido, DigSig, KMK.	Noted	Derived PIV	Note - Digital signature and key management keys are not part of derived PIV, and non-PKI DPCs such as FIDO would be invalidated by removing the linkage to the PIV account.
413	DHS	1 - Federal	Line 1129-1130	"When invalidation occurs, the issuer SHALL notify the cardholder of the change."	IAW SP800-53, when you revoke/lock an IT system account/etc., you do not inform the person the action has been taken. When it fails to work, they call in and are managed through a secure process. See comment to 1115. Recommend delete.	Declined	Derived PIV	Decline - Not aware of any prohibition in 800-53, and FIPS 201 can require this notification. Also, SP 800-63B does require this notification.
414	DHS	1 - Federal	Line 1182-1183	"MAY choose to deploy PIV Cards with electromagnetically opaque holders or other technology…"	At this point in time, MAY ought to be SHALL. This change would go a long way toward protecting the VCI for issuers who choose not to use the pairing code.	Declined	PIV Card	Decline - This is addressed in SP 800-73. As described in SP 800-73, implementing VCI without pairing code is a risk-based decision each agency has to take based on risk assessment. The text in SP 800-73 states: "A DAA's decision to approve the issuance of PIV Cards that implement the VCI without requiring the pairing code shall be based on a risk assessment that weighs the perceived benefit against the risk of unauthorized disclosure of cardholder data exposing previously contact-restricted X.509 certificates to skimming. The previously contact-restricted X.509 certificates include information about the cardholder such as name and email address. Compensating controls shall be captured in the appropriate system security plan."
415	DHS	1 - Federal	Line 1205-1207	"The PIV cardholder interacts with these components to gain physical or logical access to the desired federal resource."	Should be "The PIV cardholder interacts with these components for PIV card management activities, and to gain physical or logical access to authorized federal resource."	Duplicate	PIV Card	Duplicate of issue #420
416	DHS	1 - Federal	Line 1212	"...directories and certificate status servers. This subsystem also..."	Recommend adding "...directories and certificate status servers. This subsystem depends on the PIV Front-End Subsystem to interact with the PIV card during issuance and management activities. This subsystem also…"	Declined	Other	Decline - The text that was commented on was not intended to describe the relationship between the different subsystems.
417	DHS	1 - Federal	Line 1212-1213	"…the binding and termination…"	Other parts of this draft use "…the binding, issuance, and termination…". Recommend adding issuance for consistency.	Accept	Other	Accept - While derived PIV credentials are not necessarily issued (e.g., in the case of non-PKI derived PIV credentials), they would be in the case of PKI-based DPCs. We will add "issuance" to cover the PKI case.
418	DHS	1 - Federal	Line 1215-1216	"The physical and logical access control systems, protected resources, and authorization data."	Recommend "The physical and logical access control systems, and their authorization data, that interact with the PIV Front-End Subsystem components to protect federal facilities, networks, and systems."	Declined	Other	Decline - This text wasn't intended to describe the interconnection of components.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
419	DHS	1 - Federal	Line 1220-1221	Figure 3-1 is hugely improved. PIV Relying Subsystem is not properly defined here.	PIV Relying Subsystem needs to be structured around access control systems/authorization data, not around devices. Both LACS and PACS rely on PIV Front-End Subsystem components to let someone gain access to a resource. Replace LACS bullet list with * Directory Services; *Privileged Access Services; *VPN Services. Replace PACS bullets with * PACS Host Servers; * PACS Door Controller Panels.	Declined	Other	Decline - The existing text already addresses authorization data, but was not intended to address specific technologies or product classes.
420	DHS	1 - Federal	Line 1222-1223	"The PIV Front-End Subsystem in Figure 3-1 consists of credentials and devices that are used during authentication."	Recommend "The PIV Front-End Subsystem in Figure 3-1 consists of credentials and devices that are used during card issuance, authentication, and card lifecycle management."	Accept in Principle	Other	Accept in Principle - While the PIV Front-end subsystem is not used for management, we will relocate discussion of PIV card lifecycle management from Section 3.1.1 to 3.1.2.
421	DHS	1 - Federal	Line 1225	"...credentials might also be registered after…" it is very unclear what registered means. In FIPS 201 terms, registration is part of identity proofing."	Recommend "credentials might also be bound, issued, and managed after…"	Accept	Enrollment	Accept - agree with new language
422	DHS	1 - Federal	Line 1227	"...with one or more embedded Integrated Circuit Chips (ICC)…"	Recommend this policy be changed to single chip dual-interface cards. "...with one embedded Integrated Circuit Chip (ICC)…" This policy enables hybrid cards with 125KHz which is inherently insecure and not part of SP800-116 anymore. The PIV in E-PACS does not support this configuration, and the GSA APL does not test/affirm it as PIV compliant."	Duplicate	PIV Card	Duplicate of issue #432 - although for another line number.
423	DHS	1 - Federal	Line 1251-1252	"Biometric capture devices may be located at secure locations where a cardholder may want to gain access." They are also used as part of the ID Proofing and Registration process for card lifecycle management, not just access control.	Recommend the following... "Biometric capture devices are part of the identity proofing and registration process that supports the PIV Issuance and Management Subsystem. They are also located at secure portals of entry where a cardholder may want to gain access."	Accept in Principle	Authentication	Accept in Principle - Section 3.1.2 has been updated to include when biometric capture devices are appropriate.
424	DHS	1 - Federal	Line 1262-1263	"...physical (visual surface) and logical (contents of the ICC)…" More than logical credentials are put on the card. Also includes printed surface, person identifiers, PACS credentials, facial image, etc.	Recommend "...physical (visual surface) and electrical (contents of the ICC)…"	Declined	PIV Card	Declined - Logical content is more than what is listed in the suggested change. It includes anything in the ICC.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
425	DHS	1 - Federal	Line 1276-1278	"It is where the relevant cardholder attributes are maintained. The IDMS creates the PIV account and associates the cardholder's PIV Card and derived PIV credentials with the account. The account…" The word account really does not work here, per previous comments. This is not an account you login to and use. Rather, an identity record is established and maintained with PIV/Derived PIV information via Enterprise IDMS.	Recommend… "It is where the relevant cardholder attributes are maintained. The IDMS creates the identity account and associates the cardholder's PIV Card and derived PIV credentials with the identity record. The identity record..."	Declined	Enrollment	Decline - However changes were made that address issues related to this in issue #492, we use the term IDMS to refer to the collection of records, which may be split across multiple components. We will rephrase the term PIV Account to PIV Identity Account to distinguish it from application/system accounts.
426	DHS	1 - Federal	Line 1296-1297	"...associated with a file on a computer system." This is LACS only. Recommend adding PACS.	Recommend "...associated with a file on a computer system, or a secure portal (E-PACS controlled) within a facility."	Accept	Authentication	Accept - Will add the additional text recommended.
427	DHS	1 - Federal	Line 1309-1337	Seven card lifecycle activities listed - PIV Card Destruction not in the list.	Recommend adding an additional lifecycle activity for PIV Card Destruction and update Figure 3-2	Declined	PIV Card	Decline - It is already covered in line 1345.
428	DHS	1 - Federal	Line 1315-1317	"PIV Card Request: The initiation of a request for the issuance of a PIV Card to an applicant and the validation of this request." As it stands, it does not explain who is authorized to fulfill this request.	Recommend explicitly stating that the "Registrar" is the authorized entity required to approve a "PIV Card Request," and validate the requirement (e.g., authorized adjudicative entity, personnel security entity).	Declined	Enrollment	Decline - The term registrar was used in prior version of the FIPS 201 and has been removed in revision 2 given comments that the term is confusing and given agency have different name/title for the role.
429	DHS	1 - Federal	Line 1323	"Personalization (physical and logical)…"	Recommend "Personalization (printed and electrical)…" because it is more than logical information. Also supports physical.	Duplicate	PIV Card	Duplicate of issue #424
430	DHS	1 - Federal	Line 1326	"Generation of logical credentials…"	Recommend for consistency with line 1333 "Generation of PKI credentials…"	Accept	PIV Card	Accepted
431	DHS	1 - Federal	Line 1352-1353	"For example, physical access systems are not usually well-suited for a federation protocol."	The market/technology for PACS is changing and this statement may no longer be true. It is not a necessary statement, so recommend deleting it. It is limiting on how PACS may be implemented.	Accept in Principle	PIV Federation	Accept in Principle - document text has been re-word to " physical access systems tend not to use federation protocols and instead rely on direct authentication"

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
432	DHS	1 - Federal	Line 1369-1371	"The PIV Card SHALL comply with the physical characteristics described in [ISO 7810], [ISO 10373], and [ISO 7816] for contact cards in addition to [ISO 14443] for contactless cards."	Recommend now being explicit about dual-interface, not dual-chip. The market truly has decided this issue regarding certified PIV card stock. Also, ISO 10373 applies equally to contact and contactless, not just contact. ISO14443 Type A vs Type B should also be recognized. This dramatically impacts reliability in the field. The market has clearly determined Type A. Recommend... "The PIV Card SHALL be a dual-interface card. It SHALL comply with the physical characteristics described in [ISO 7810], and [ISO 7816] for contact cards, and [ISO 14443] Type A for contactless cards. It shall comply with [ISO 10373] test methods for both contact and contactless interfaces."	Declined	PIV Card	Decline - FIPS 201 is inclusive of both dual and single chip implementations and should not further restrict possibly legitimate card chip configuration. Changes to chip type/communication is addressed in SP 800-96. See also #438 for line 1466-1467
433	DHS	1 - Federal	Line 1397	"The PIV Card SHALL contain a contact and a contactless ICC interface."	Per prior comment on 1369-1371, recommend being explicit: "The PIV Card SHALL be a dual-interface card with a single chip, a contact and a contactless ICC interface."	Duplicate	PIV Card	Duplicate of issue #432
434	DHS	1 - Federal	Line 1421-1422	"Cards SHALL NOT malfunction or delaminate after hand cleaning with a mild soap and water mixture."	This is the only requirement that was tested as part of the NVLAP supported GSA APL test program. Manufacturers guarantee their cards, including the laundry test. This requirement adds no value to the actual PIV card. The manufacturer's card body (subject of the requirement) is not the real problem here. More likely it will be issues with things like color fading and peeling laminate, not the card body itself. Recommend deleting this requirement.	Declined	PIV Card	Decline - It is important to keep it in the Standard - as described. The test is being done by manufacturer.
435	DHS	1 - Federal	Line 1442-1443	Departments and agencies MAY choose to punch an opening in the card body to enable the card to be oriented by touch or to be worn on a lanyard.	Punching a card to use a lanyard or for tactile card orientation is strongly discouraged by manufacturers and most issuers do not do it. This language does not match current practices within the PIV card domain. If you do punch a PIV card, and the hole avoids the contactless antenna, you will punch part of the security elements that are printed for an individual on their PIV card (e.g., goes through facial image). Recommend deleting this language.	Declined	PIV Card	Declined - This was requested by US Access Board on FIPS 201-2 revision (comment keyword USAB-4) Punching a hole is at agencies discretion - other methods for 508 compliance are also a possibility in FIPS 201.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
436	DHS	1 - Federal	Line 1458	"The PIV Card MAY be subjected to additional testing." This is is an open ended requirement that can not be met by manufacturers/issuers alike.	What is the intent of the statement? That FIPS 140 applies? NPIVP? Anything else? FPKIPA or APL testing? None of these have anything to do with the manufacture of the card or specifications on interaction with the ICC. Not clear why this is needed in FIPS 201. Recommend delete.	Accept	PIV Card	Accept - Agree to delete.
437	DHS	1 - Federal	Line 1463	"Logically stored..." is no longer accurate	Recommend "Electrically stored…" for specific reference to the ICC.	Declined	PIV Card	Decline - Logical content is more than what is listed in the suggested change. It includes anything in the ICC. Similar to issue #424
438	DHS	1 - Federal	Line 1466-1467	"This Standard does not specify the number of chips used to support the mandated contact and contactless interfaces."	The market clearly indicates a single chip dual-interface strategy. Recommend delete for consistency with comments to 1369-1397. In particular, PIV is implemented with a single, dual interface chip. That is the key. Adding 125KHz is outside the PIV domain and should remain that way.	Duplicate	PIV Card	Duplicate of issue #432 but for another line number.
439	DHS	1 - Federal	Line 1473-1479	"The reason for the recommended reserved areas is that placement of the embedded contactless ICC module may vary between manufacturers, and there are constraints that prohibit printing over the embedded contactless module. The PIV Card topography provides flexibility for placement of the embedded module, either in the upper right corner or in the lower portion. Printing restrictions apply only to the area where the embedded module is located."	There should be a single reserved area for the chip/contact plate per 7810. This standard really should no longer encourage 125KHz for PACS or other dual-chip designs.	Duplicate	PIV Card	Duplicate of issue #432 which comments on a separate line number in the document.
440	DHS	1- Federal	Line 1601-1604	Agency Seal; if used	Recommend use of an agency seal is REQUIRED - not a CONSIDERATION	Accept in Principle	PIV Card	Accept in Principle - Language will be updated to indicate inclusion of the agency seal may be required by future editions of this specification.
441	DHS	1 - Federal	Line 1701	"…Logical Characteristics"	Is actually "…Electrical Characteristics" Actually, for consistency, this should line up with SP800-73 which calls this the ""PIV Card Data Model"" as stated at line 1710."	Declined	PIV Card	Decline - Logical content is more than what is listed in the suggested change. It includes anything in the ICC. Similar to issue #424
442	DHS	1 - Federal	Line 1760	"A CHUID MAY also include a Cardholder UUID…"" A CHUID may include a CHUUID.	"A CHUID MAY also include a Person UUID…" This makes it clear it is a Person Identifier, much like the PI in the FASC-N.	Duplicate	PIV Card	Duplicate of issue #358

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
443	DHS	1 - Federal	Line 1765	"The FASC-N, card UUID, and expiration date SHALL NOT be modified post-issuance."	This is missing a key data element. Just like the PI within the FASC-N, the Cardholder (Person) UUID shall not be modified post issuance. "The FASC-N, Card UUID, Cardholder UUID, and expiration date SHALL NOT be modified post-issuance."	Accept	PIV Card	Accept - Document text was updated to "...expiration date, and, if present, the cardholder UUID, SHALL not be modified post-issuance"
444	DHS	1 - Federal	Line 1789	"Symmetric card authentication key"	This is a requirement to the benefit of a single vendor in the E-PACS marketplace. It is not cross-agency interoperable. It is not tested by the GSA APL because key management is unknown and a testing harness is not feasible. This method is not widely used. Asymmetric performance on PIV cards with E-PACS is similar to that of symmetric authentication. This mechanism should be DEPRECATED in this version of the standard. This will further enhance interoperability across all agencies for use of the PIV card.	Noted	Authentication	Note - Related to issue #207
445	DHS	1 - Federal	Line 1826-1827	"Symmetric cryptographic operations are not mandated for the contactless interface, but departments and agencies MAY choose to supplement the basic functionality with storage for a symmetric card authentication key and support for a corresponding set of cryptographic operations. For example, if a department or agency wants to utilize an Advanced Encryption Standard (AES) based challenge/response for physical access, the PIV Card SHALL contain storage for the AES key and support AES operations through the contactless interface."	See comment on line 1789. This language should be deprecated or removed.	Noted	Authentication	Noted - Cited text is no longer in the draft specification; it was in section 4.2.2 of FIPS 201-2
446	DHS	1 - Federal	Line 1840-1842	"The card UUID SHALL be encoded as a Uniform Resource Name (URN), as specified in Section 3 of [RFC 4122]." Missing an important UUID.	Cardholder (Person) UUID is critical for future activities in federation. This data element should be mandatory, not optional. "The card UUID SHALL be encoded as a Uniform Resource Name (URN), as specified in Section 3 of [RFC 4122]. The mandatory Person UUID, shall be encoded as a Uniform Resource Name (URN), as specified in Section 3 of [RFC 4122]."	Duplicate	PIV Card	Duplicate of issue #592
447	DHS	1 - Federal	Line 1843-1848	"The PIV authentication certificate MAY include a PIV background investigation indicator (previously known as the NACI indicator) extension (see Appendix B.2). This non-critical extension indicates the status of the cardholder's background investigation at the time of card issuance."	"This non-critical extension is never evaluated by relying party systems. To date, no issuance system does a post-issuance update when the status flips from partial to full investigation complete. This extension is outdated and should be removed from the standard."	Noted	PIV Card	Noted - The NACI indicator is being deprecated (see line 2957).

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
448	CertiPath Inc.	2 - Industry	4.1.4.3 Line 1605-1619	Revised language makes placement of the Federal Emergency Response Official banner ambiguous. Note opening sentence "If used as the federal emergency response official identification label. . ." Assuming consistency in placement of this label is still expected, this section should start with a statement to that effect and then provide the additional language for situations where this designator is not required. Also, isn't it time to mandate white on red?	Recommend revising language so that it is clear that when a card needs to indicate Federal Emergency Response Official, it is in Zone 12F. Also, consider requiring white on red except for extenuating circumstances (if there are any).	Accept in Principle	PIV Card	Accept in Principle - Text was updated to clarify use of PIV Card to Identify Federal Emergency Reponses officials.
449	CertiPath Inc.	2 - Industry	4.2.1 Line 1745	Typo: mechanism is misspelled	Correct spelling of mechanism.	Accept	Editorial	Accept - Typo in text was updated
450	CertiPath Inc.	2 - Industry	4.2.1 Line 1761-1762	Sentence beginning "The value of the cardholder UUID. . ." needs revision to ensure accuracy and clear understanding. At a minimum, there needs to be an article (a, the) before "valid" and replace 'a' in front of "16 byte" with 'the' as there is only one correct encoding of a UUID.	Consider revising this sentence: "The value of the cardholder UUID SHALL be the 16 byte binary representation of a valid UUID, as specified in [RFC 4122]".	Accept	Editorial	Accept - The proposed change here is simply to change"**a** 16 byte binary representation" to "**the** 16 byte binary representation." Accept as an editorial comment.
451	CertiPath Inc.	2 - Industry	4.2.2 Line 1790	If deprecated, is it still optional?	Consider revising the statement concerning the SYM-CAK	Declined	Authentication	Decline - Key was optional in FIPS 201-2, deprecated and optional seems like the right next step before making it go away entirely.
452	CertiPath Inc.	2 - Industry	4.2.2 Line 1802-1804	Formatting error - PIV Secure messaging key header is stuck on the end of PIV Card application administration key explanation	Fix formatting error.	Duplicate	Editorial	Duplicate of issue #205
453	CertiPath Inc.	2 - Industry	5.2.1 Line 2100	This statement should include the digsig certificate, since this should be generated on card, never exported and would therefore die with the card.	Revise to include digsig certificate.	Declined	PIV Card	Decline - This is out of scope for FIPS 201 and is more of an issue for the certificate policy.
454	CertiPath Inc.	2 - Industry	5.4 Line 2111-2114	This imposes a fundamental change on agency implementations, particularly for organizations that operate their own PKI domains and do not use COMMON policy OIDs for their digsig or kmk certificates. This section previously stated "This specification imposes no requirements on digital signature or key management certificates issued by legacy PKIs." In addition, COMMON Policy takes its requirements from FIPS 201-3 for the implementation of PIV certificates. This is necessary because at the end of the day FIPS 201 trumps COMMON Policy. If FIPS 201-3 does not allow something, there is no avenue or justification for FPKI/COMMON policy to do so.	"Restore Legacy PKI to FIPS 201-3 to ensure clarity and permit continued use of alternative digsig and kmk policy OIDs. Alternatively, revise language on lines 2091-2097 to replace ""SHALL"" with ""SHOULD"" and add a footnote to indicate that agencies that operate legacy PKI may choose to use alternate policy OIDs for digsig and kmk. "	Duplicate	Other	Duplicate of issue #241

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
455	CertiPath Inc.	2 - Industry	6.1.1 Line 2179-2181	It would seem more correct to reference HSPD-12 and M-19-17 here, since those two documents are Federal Identity Policy and do provide the justification for the existence and continuing existence of FIPS 201	Reconsider removal of Section 6.1.1	Accept in Principle	Other	Accept - Update has expanded on the relationship between FIPS 201, M-19-17 and HSPD-12.
456	CertiPath Inc.	2 - Industry	6.2.3.1 Line 2268	This is a list of steps in authenticating using PIV-AUTH. As such, use of "previously issued" in the bullet starting on line 2268 is unnecessary	Consider revising this bullet to remove "previously issued"	Accept	Authentication	Accept - Minor editorial cleanup.
457	CertiPath Inc.	2 - Industry	7.3 Line 2496-2498	See previous comment. Use of the term 'recommended' here may provide a false sense of necessity to agency readers. There are certainly times when the federated approach is warranted, but there are also times when the direct use of the PIV credential makes more sense. This section speaks to the Benefits of Federation but fails to discuss any of the drawbacks or vulnerabilities. In addition there is no parallel discussion of the Benefits of directly trusting PIV credentials.	Revise this section to remove the term 'recommended' and discuss federation as a viable alternative to direct trust but not the 'preferred' method.	Duplicate	PIV Federation	Duplicate of issue #385
458	DHS	1 - Federal	Line 1860-1861	"The card UUID SHALL be encoded as a Uniform Resource Name (URN), as specified in Section 3 of [RFC 4122]." Missing an important UUID.	cardholder (Person) UUID is critical for future activities in federation. "The card UUID SHALL be encoded as a Uniform Resource Name (URN), as specified in Section 3 of [RFC 4122]. The mandatory Person UUID, shall be encoded as a Uniform Resource Name (URN), as specified in Section 3 of [RFC 4122]."	Duplicate	PIV Card	Duplicate of issue #592
459	DHS	1 - Federal	Line 1865-1868	Symmetric Card Authentication Key	Should be deprecated. See comment to 1789.	Noted	Authentication	Noted - Document clearly says that it is deprecated.
460	DHS	1 - Federal	Line 1950-1953	"If the signature on the biometric data record was generated with a different key than the signature on the CHUID, the certificates field of the CMS external digital signature SHALL include the content signing certificate required to verify the signature on the biometric data record. Otherwise, the certificates field SHALL be omitted."	"To our knowledge, there are no issuers that use a separate biometric content signing key from the content signing key in the CHUID. Recommend deprecating this language and requiring use of the content signing key in the CHUID."	Accept in Principle	PIV Card	Accept in Principle - We can not prohibit use of a different key in this revision, however updated text will include stronger language and indicate it may be required in subsequent revisions.
461	DHS	1 - Federal	Line 1972-1974	"The two types of identifiers that serve as identification (of the cardholder) for authentication and authorization purposes are as follows:" The sentence is missing identifier for the card itself.	"The two types of identifiers that serve as 1) identification (of the person), and 2) identification (of the card), for authentication and authorization purposes are as follows:"	Declined	PIV Card	Decline - The ultimate goal is to identify the cardholder. The card identifiers are intended to indirectly identify the cardholder.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
462	DHS	1 - Federal	Line 1997-1999	"Examples include the cardholder UUID that may appear in the CHUID or the subject names that may appear in the subjectAltName extension in the PIV authentication certificate." Missing the Person UUID and FASC-N OI/PI values.	"Examples include the cardholder UUID that may appear in the CHUID or the subject names that may appear in the subjectAltName extension in the PIV authentication certificate."	Declined	PIV Card	Decline - SP 800-73 specifies which values are recognized in the FASC-N (which does not include the OI/PI values). And the cardholder UUID is already referenced as a cardholder identifier.
463	DHS	1 - Federal	Line 2010-2012	Issue is not enforceable by the card.	Recommended language: "The PIN should not be easily guessable. The PIN SHALL be a minimum of six digits and a maximum of eight digits in length. The PIV Card SHALL provide a policy that supports a list of chosen PINs (minimum of 100) that shall be rejected. The PIV card SHALL enable the list of chosen PINs to be set by the CMS, enabling the Issuer to control their list of chosen PINs that should be rejected. This PIN policy shall be discoverable and defined in [NIST SP 800-73]."	Duplicate	Authentication	Duplicate of issue #589
464	DHS	1 - Federal	Line 2032-2039	Contactless Reader Requirements	Recommend adding "Contactless Readers may conform to Near-Field Communications (NFC) standards." This will greatly expand usage of Derived PIV in the mobile device market.	Declined	Derived PIV	Decline - FIPS 201 cites specific standards. Section 4.4.2 references ISO 14443 and ISO 7816 which cover NFC standards.
465	DHS	1 - Federal	Line 2046-2047	"When the PIV Card is used with a PIN or OCC data for physical access, the input device SHALL be integrated with the PIV Card reader." It is not clear what is sought by this statement. A) the fingerprint reader is an integral part of a reader housing the contact/contactless reader; B) a separate fingerprint reader is cabled to a contact/contactless reader. Equally true is replace ""fingerprint reader"" with ""PIN pad"". The market has both environments. They can be very modular in nature.	Clarify the intent, or remove the requirement.	Accept in Principle	Other	Accept in Principle - Update will clarify the intent of the requirement for input devices to be integral to readers. Add to Paragraph 3, Section 4.4.4.
466	DHS	1 - Federal	Line 2103-2106	"However, a PIV authentication or card authentication certificate MAY be revoked and subsequently replaced without revoking the PIV Card." This is confusing. I think it is trying to say you can revoke a PIV card certificates for an individual, but their Enterprise IDMS (or maybe CMS) record is still in good standing and the individual is still eligible for new PIV/CAK auth certificates or a new PIV card.	Is "revoking the PIV card" any different from "invalidating the PIV card"? This may best be discussing PIV card eligibility at the Enterprise IDMS because that directly affects Derived PIV. Please clarify.	Declined	Other	Decline - The term "revoke" is appropriated when referring to the PIV card itself (as opposed to the certificates). In particular, the sentenced referenced by this comment is clear by including a forward pointer to Section 2.9.1, which describes the revocation process for reissued cards.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
467	DHS	1 - Federal	Line 2130	[No comment]	Recommend saying "…in accordance with Department/Agency Certification Practices Statement."	Declined	Other	Decline- Revocation procedures may be specified multiple places- we don't need to call out any single document.
468	DHS	1 - Federal	Line 2135-2136	"...SHALL NOT be distributed publicly (e.g., via HTTP accessible from the public internet)." Is really open to interpretation for the intent of the requirement. Is it OK for a department/agency to publish PIV Auth/Card Auth on a public directory that is only accessible within the department/agency? If one considers APT, this may be leaking information.	Recommend strengthening the language. "...SHALL NOT be distributed over the public internet nor throughout an agency/department (e.g., via HTTP accessible directory)."	Declined	Other	Decline - The text proposed in the comment is quite broad, and would preclude legitimate use cases involving certificate directories.
469	DHS	1 - Federal	Line 2187	PIV Card Authentication Mechanisms	This section is missing the use of Secure Messaging as a valid authentication method. It is cryptographically secure and provides the Card UUID within the CVC for authorization decisions. Recommend adding Secure Messaging as an authentication method within FIPS 201-3.	Noted	PIV Card	Noted - Section 6.2.3.3 allows Authentication Using Secure Messaging Key (SM-AUTH)
470	DHS	1 - Federal	Line 2196	"...following CTC authentication using a PIN supplied by the cardholder." Prior language in the standard enables use of OCC for the CTC to activate the card, enabling access to all three biometric modalities for off-card comparison.	Recommend "...following CTC authentication using OCC or a PIN supplied by the cardholder."	Duplicate	Authentication	Duplicate of issue #471.
471	DHS	1 - Federal	Line 2207	"...for presentation of the PIN and acquisition of a biometric sample" Missing OCC option.	Recommend being explicit if OCC is not valid to activate the card in this scenario.	Declined	Authentication	Decline - OCC is not envisioned to be used to unlock a card to release a biometric template, but there is no compelling reason to prohibit this (as that might require additional logic on the card).
472	DHS	1 - Federal	Line 2216-2217	As written, this method does not confirm if the card is revoked.	Add new bullet: "The PIV Auth cert is read from the card. Confirm this certificate is not revoked or expired."	Declined	Authentication	Declined - Requiring revocation check would not be backward-compatible (section 1.3.2) with install base and readers available on the GSA approved products list.
473	DHS	1 - Federal	Line 2223-2237	As written, this method does not confirm if the card is revoked.	Recommend adding "Some characteristics…" to this section.	Duplicate	Authentication	Duplicate of issue #472
474	DHS	1 - Federal	Section 2 and 3	Destruction of a PIV card. Nothing stated about recording the destruction act to the CMS, to support cradle to grave issuance activities.	Recommend establishing controls requiring the destruction act/event be reported/recorded as part the issuance activities to maintain accounting of all issuance processes.	Accept in Principle	PIV Card	Accept in Principle - Text was updated to reflect requirement to update CMS with information on card termination and method of termination.
475	DHS	1 - Federal	Line 2316-2340	SYM-CAK	SYM-CAK should be deprecated. See comment to 1789.	Noted	Authentication	Note - Sym-CAK has been deprecated in FIPS201-3

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
476	DHS	1 - Federal	Line 2323-2325	This requirement highlights that there are too many expiration dates on the card. Which are for the card? Which for the authentication mechanism?	Sym-CAK is deprecated, yet this comment still applies to other authentication methods. Certificates do not inform if a card is expired. That information is only in the CHUID expiration date field. This should not be used/recommended by this standard. Certificates shall expire on or before the card. These are the expiration dates critical to the operation of an access control system. The CHUID and card expiration should not be referenced here, nor in all PKI driven authentication methods supported by the PIV card.	Accept in Principle	Authentication	Accept in Principle - Updated text replaces the first bullet in Section 6.2.4 with the first bullet in Section 6.2.1.1, saying: The CHUID or another data element is read from the card. The signature of the CHUID or another data element is verified to ensure that the card has not expired and that the card comes from a trusted source. With the footnote: The PIV authentication certificate or card authentication certificate may be leveraged instead of the CHUID to verify that the card is not expired.
477	DHS	1 - Federal	Line 2335-2340	Does not discuss interoperability.	Recommend adding a bullet "Is not cross agency interoperable and generally will not work with PIV cards issued by another agency.	Declined	Authentication	Decline- that is out-of-scope for the characteristic bullets, but is a major part of the reason we are deprecated SYM-CAK in FIPS 201-3.
478	DHS	1 - Federal	Line 2430-2440	Introducing PAL is inconsistent with the model offered by SP800-63B.	Recommend only using AAL from SP800-63B in this context. It maps very well for Physical Access.	Declined	Authentication	Decline - The properties and requirements for physical access do not naturally align with logical access control. However, the final version of FIPS 201-3 does not define Physical Assurance Levels and instead merely describes the assurance characteristics of the applicable PIV authentication mechanisms for physical access use cases. Further guidance will be developed in a revision to NIST SP 800-116
479	DHS	1 - Federal	Line 2430-2440	Why is PAL being introduced? 800-63 addresses this	See comments to line 2430-2440.	duplicate	Authentication	Duplicate of issue #478
480	DHS	1 - Federal	Line 2430-2440	§6.3.1 PAL concept is not consistent with SP800-63B. Recommend aligning FIPS 201-3 with ICAMSC Playbooks with SP800-63-B with PIV in E-PACS with GSA APL testing program with SP800-116, and industry capabilities.	See comments to line 2430-2440.	Noted	Authentication	Noted - The properties and requirements for physical access do not naturally align with logical access control. As such, the SP 800-63B authenticator assurance levels cannot be directly applied to physical access use cases. While Draft FIPS 201-3 initially specified Physical Assurance Levels, The final version of FIPS 201-3 instead merely describes the assurance characteristics of the applicable PIV authentication mechanisms for physical access use cases. Further guidance will be developed in a revision to NIST SP 800-116.
481	DHS	1 - Federal	Line 2449-2450	Table 6-1 does not conform with SP800-63 AALs using multi-factor authentication (something you know, something you have, something you are)	Industry does not follow the paradigm listed in this table. Recommend aligning with industry and using multi-factor authentication paradigm defined in SP800-63B.	Declined	Authentication	Decline - The properties and requirements for physical access do not naturally align with logical access control. However, the final version of FIPS 201-3 does not define Physical Assurance Levels and instead merely describes the assurance characteristics of the applicable PIV authentication mechanisms for physical access use cases. Further guidance will be developed in a revision to NIST SP 800-116

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
482	DHS	1 - Federal	Line 2460-2461	Table 6-2 does not conform with SP800-63 AALs using multi-factor authentication (something you know, something you have, something you are)	Industry does not follow the paradigm listed in this table. Recommend aligning with industry and using multi-factor authentication paradigm defined in SP800-63B.	Accept in Principle	Authentication	Accept in Principle - Tables have been revised to create 3 separate tables (Physical Access-Table 6.1, Remote Network access - Table 6.2, Local Workstation Access -Table 6.3). Table 6.2 is aligned with SP 800-63B while the other tables are not aligned (because are not remote network methods) but show the degree of assurance provided. We did not accept the recommended changes. See comment #481.
483	DHS	1 - Federal	Line 2472-2474	"The IdP SHALL associate this login with the PIV account of the cardholder and SHALL create an assertion representing the cardholder to be sent to the RP, including attributes of the cardholder stored in the PIV account."	See comment on lines 1332-1334. The IdP is likely not the Enterprise IDMS that issued the credential. The IdP will have an attribute store associated with an identity. The PIV cardholder is not "logging in" per se to the IdP, they are authenticating their identity using their PIV card for access to the resource controlled by the RP. This should be clarified.	Accept in Principle	PIV Federation	Accept in Principle - Updated text uses clearer terminology when referring to authentication actions.
484	DHS	1 - Federal	Line 2504-2506	Stable Identifier	While it is true an IdP can establish its own unique identifier for a given identity, this may not be to the advantage of the federal enterprise. A PIV card has both OI/PI from the FASC-N, as well as the Cardholder (Person) UUID. The Person UUID is uniquely suited to this task, as it spans any issuer, any IdP, and any RP evironment, with no risk of collision. Recommend adding language about using the PIV Person UUID as a stable identifier within any federation model serving the PIV market.	Declined	PIV Federation	Decline - Cardholder UUID is not a required element that the IDP can depend on.
485	DHS	1 - Federal	Line 2509	"...tasked to the credential issuer/IdP."	Recommend this only refer to the IdP, even though the CSP may be the IdP.	Accept in Principle	PIV Federation	Accept in Principle - Updated text only refers to processes allocated to IdP
486	DHS	1 - Federal	Line 3063-3064	PAL not consistent with SP800-63B.	Recommend delete in favor of AAL from SP800-63B.	Duplicate	Authentication	Duplicate of issue #478
487	DHS	1 - Federal	[none given]	Secure Messaging should be added as a new authentication method for high performance cryptographic single factor.	[blank]	Noted	Authentication	Noted - See section 6.2.3.3, lines 2304-2315, for details on the SM-AUTH authentication method.
488	DHS	1 - Federal	[blank]	Clarify that 1:1 biometric verification is the generic concept. This would enable defining Fingerprint, Facial, and Iris, as the modalities, no matter if on or off card, that comply with the requirement for biometric verification.	[blank]	Noted	Authentication	Noted - 1:1 biometric comparison in the various modality is well covered in the standard.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
489	DHS	1 - Federal	[blank]	800-156 defines the Enrollment Record and a structure used to transfer enrollment information between agencies. Recommend consideration of Secure Identity data exchange from the Secure Identity Alliance (https://secureidentityalliance.org/). This would extend SP800-156 which would include credential information, attribute information, and related. This expansion would greatly improve vendor uptake, and inter-agency transfers and reciprocity.	[blank]	Declined	Enrollment	Decline - Out of scope for FIPS 201, but could reconsider for SP 800-156.
490	DHS	1 - Federal	[blank]	Promote and sponsor a discussion about Person Identifiers for credentialing, authentication, and in particular, federation. Specifically FASC-N OI/PI, Cardholder (Person) UUID, attributes about what type of person (contractor, foreign national, employee, state/local, federal, etc.)	[blank]	Noted	Other	Noted - Discussion proposed is outside the scope of FIPS201 document. Use of Person identifiers will be addressed in Federation SP.
491	CISA	1 - Federal	1 pg 1, LIne 324	Provide reader with reference to related content within document	A footnote note here referencing the dependencies that are outlined in Section 6.3 is in order.	Declined	Editorial	Decline - Footnote is note appropriate
492	CISA	1 - Federal	1.2 +F5:I19pg 2: Line 364	the assumption here that the Agency IDMS responsible for card issuance is the Agency “operational” Identity Management system is usually not correct.	Add line "This IDMS interfaces with other Agency Identity and Access Management services that enable the management of identity information throughout the lifecycle of the Identity."	Declined	Enrollment	Decline - How agencies organize and implement their architectures is up to individual agencies- the records in the PIV Identity Account may be split across multiple components, but collectively, those components act as an IDMS.
493	CISA	1 - Federal	1.3.4 pg 4: Line 420	No date specified for use of CHUID authentication	Specify a specific date after which CHUID authentication will be discontinued.	Accept in Principle	Authentication	Accept in Principle - Updated text clarifies when new, optional and removed features/mechanisms will go into effect. This is also related to #339 on the effective date of FIPS 201-3 in general.
494	CISA	1 - Federal	1.3.5 pg: Line 422	None of the other forms of authentication enable VIS as an input.	[blank]	Noted	Authentication	Noted - The current text states that future revisions may remove VIS, it is not ideal to highlight VIS further.
495	CISA	1 - Federal	1.3.4 pg. 4: Line 425	In a manner similar to other FIPS there should be a date-certain upon which the removed feature will be discontinued.	Specify a specific date when magnetic stripe feature will be discontinued.	Duplicate	PIV Card	Duplicate of issue #387
496	CISA	1 - Federal	1.3.4 pg. 4: Line 425	Is the magnetic stripe deprecated or is the encoding of the magnetic stripe with information deprecated?	Clarify or give forward reference to where the document clarifies.	Declined	PIV Card	Decline - Magnetic stripe is just being referenced as an example. Section 4.1.4.4 is clear that the magnetic stripe is deprecated.
497	CISA	1 - Federal	2.1 pg. 7: para 2: Line 515	Item c. Does the FPKI practice of issuing CRLs every 18 hours and next Update of 48 hours satisfy (c) for rapid electronic authentication?	Define "rapid" in this context.	Declined	Other	Decline - Section 2.9 in FIPS 201, as well as the FPKI Common Policy Framework, specify the detailed requirements for revocation.
498	CISA	1 - Federal	2.1 pg. 7, para 2: Line 518	The list in lines 520 to 546 only relates to a & b. c & d are not addressed.	Address c & d or note that list only addresses a & b.	Accept in Principle	Other	Accept in Principle - Updated text clarifies that the PIV implementation bullets expand on the control objectives in HSDP-12, but there was not intended to be a strict mapping to control objectives.
499	CISA	1 - Federal	2.2 pg. 8, para 2: Line 550-556	How is it expected that the variations in the investigative requirement as required by the designation of position guidance be reflected in interagency federation protocols?	Consider adding a Trust Assurance Level (TAL) to accommodate the variation. TAL may be crucial element in Federation. Alternatively, eliminate this discussion in favor of specifying just Tier 1 as minimum trust for PIV holder.	Declined	PIV Federation	Decline - This is out of scope for this document and essential aspects of this request are covered in 7.2.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
500	CISA	1 - Federal	2.2 pg. 8, para 3: Line 557-559	Since minimum requirements for PIV investigations is Tier 1 in federation assurance scenarios, should the relying party only consider that the individual asserting a FAL has been adjudicated?	Clarify what assumptions a relying party may assume in federations	Declined	PIV Federation	Decline - This is out of scope for this document as it pertains to trust of attributes. See also issue #499
501	CISA	1 - Federal	2.2 pg. 9, last para: Line 569	If PIV credentialing investigative and adjudicative requirements are determined by Executive Agents what is the common expectations that can be expected without having access to the individual expectations.	Clarify. See previous two comments.	Declined	PIV Federation	Decline - The referenced text is intended to serve as a general warning that PIV issuers must stay up-to-date on policy guidance provided by OPM and OMB.
502	CISA	1 - Federal	Sec. 2.7, Pg. 13, Para. 1: Line 705-711	Is Departments and agencies synonymous with "organization". What is the process relationship of 800-63A or 800-79 or both.	If the expectation is that this meets both, state both on the same line.	Accept in Principle	Editorial	Accept in Principle - Text updates indicate the department or agency are to be inferred in relevant section of the document.
503	CISA	1 - Federal	Sec. 2.7, Pg. 13, Para. 1: Line 705-707	The reference to Identity Proofing in SP 800-63 is the government guidelines for Identity Proofing. It is unclear what the “tailoring process” in intended to mean here. SP800-63-3a does not refer to “tailoring” except in regards to NIST SP 800-53 controls and none in regards to Identity Proofing requirements. Proposed language is confusing. It essentially promotes separate requirements for the two documents and tries to explain/rationalize the differences. Recommend NIST merge the requirements rather than have separate requirements.	Recommend 201 require 800-63 IAL3 and Tier 1.	Declined	Enrollment	Decline - Per the discussions at the Business Requirements Meeting, the tailored issuance process described in Section 2.7 PIV provides a sufficient level of assurance. The on-boarding process and the background investigation mitigate the risks from not meeting all of the documentary evidence requirements from-63A.
504	CISA	1 - Federal	Sec. 2.7, Pg. 13, Para. 3: Line 712	Identity Proofing has no requirements for investigations. They are related but orthogonal. If there deems to be a need for evaluation of trust there should be a topic on that subject, the rationale for it and the measurement implications of that in the same manner that Identity Assurance is different than Federation Assurance, Trust Assurance (my words here) should be different than Identity Assurance. The attributes regarding the asserted trust could then be sent along with assertions about Identity, Authentication or Federation such that a relying party would be able to discern the entire realm of assurances that are being conveyed on part of the issuing party.	If there is a need for evaluation of trust, there should be a topic on that subject, the rationale for it and the measurement implications of that in the same manner that Identity Assurance is different than Federation Assurance, "Trust Assurance" should be different than Identity Assurance.	Declined	Enrollment	Decline - The topic of investigative requirements is the purview of OPM and OMB, not NIST. The investigation requirements, however, are a prerequisite to PIV issuance, which is why it is mentioned here.
505	CISA	1 - Federal	Sec. 2.7, Pg. 13, Para. 6: Line 719-720	"Trained staff" is too ambiguous for a standards document.	State precisely how one is to be trained or reference the Special Publication that specifies a training process practice statement that covers these other documents.	Declined	Enrollment	Decline - SP 800-79 will provide additional details.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
506	CISA	1 - Federal	Sec. 2.7, Pg. 13, Para. 6: Line 721-723	In what manner is the term “bound” used here?	Specify what is meant and how that is evidenced.	Accept in Principle	Enrollment	Accept in Principle - Document was updated to split this sentence into two. Replace "bound" with language indicating evidence documents shall correspond to the applicant.
507	CISA	1 - Federal	Sec. 2.7, Pg. 13, Para. 6: Line 721-723	"… SHALL NOT be expired or cancelled.”	Replace with “SHALL neither be used past their displayed expiration date nor be marked as “cancelled”.	Declined	Editorial	Decline - Existing text is more broad than proposed text.
508	CISA	1 - Federal	Sec. 2.7, Pg. 15 last Para.: Line 760	The introduction of a “compensating control” via a background investigation conflates the term IAL with another vector (background investigation) that is not referenced in that Special Publication. The source publication, SP 800-63, should be the document that indicates how compensating controls can be applied in order to elevate lack of evidence from less than IAL3 to IAL3. It is NOT the case that ONLY PIV card issuance will have this delta and unless there is a way to convey the existence of said compensating control (say by the addition of a “trust” assurance level attribute), the replying party cannot reasonably be expected to accept that an IAL3 is truly as the guidance states.	Allow use of IAL3 (as defined in SP 800-63) or modify 800-63 to allow the use of Trust (Tier 1) to compensate .	Declined	Enrollment	Decline - Per the discussions at the Business Requirements Meeting, we believe the current issuance process for PIV provides a sufficient level of assurance. We believe the on-boarding process and the background investigation mitigate the risks from not meeting all of the documentary evidence requirements from-63A.
509	CISA	1 - Federal	Sec. 2.7, Pg. 15, Para. 2: Line 768	Is this an elaboration on the SHALL statement of line 707-709 and 710-711 or is this a redundant statement?	Clarify	Declined	Editorial	Decline - This is a separate requirement.
510	Secure Technology Alliance	2 - Industry	2.3 Line 581/582	Make language more definitive	"This collection is not necessary for applicants who have a completed and favorably adjudicated Tier 1 or higher federal background investigation on record that can be located and biometrically matched to original referenced biometric used to conduct this investigation."	Declined	Editorial	Decline - Requirement already in Section 2.8.2 (line 875 in current document).
511	CISA	1 - Federal	Sec. 2.7, Pg. 15, Para. 3: Line 772	Identity Proofing requirements are specified in NIST SP 800-63-3. The meaning of the term “registration” is unclear in this section where Identity Proofing is the sole activity occurring.	Remove term or clarify	Declined	Enrollment	Declined - The term is defined in glossary.
512	Secure Technology Alliance	2 - Industry	2.4 Line 593-595	Make language more definitive	Two fingerprints for on-card comparison (OCC). These fingerprints MAY be taken from the full set of fingerprints collected in Section 2.3 and SHOULD be imaged from fingers. The fingerprint templates stored on the PIV for off-card one-to-one comparison can not be used for on-card comparison. Clarify that two different fingers are required.	Declined	Editorial	Decline - SP800-76 Section 5.4 defines requirements for fingerprints used.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
513	CISA	1 - Federal	Sec. 2.10.1, Pg. 24, Para. 2: Line 1106	Conditions when AAL2 is appropriate are vague.	Recommend adding more elaboration regarding “depending on the security characteristics of the authenticator."	Accept in Principle	Derived PIV	Accept in Principle - Updated text specifies use of Derived PIV credentials that meet AAL2 or AAL3 requirements.
514	Secure Technology Alliance	2 - Industry	2.5 Line 631-633	"With latest NIST facial recognition test surpassing both Iris and finger, it should be an alternate not secondary"	The electronic facial image is a alternate means of authentication during operator-attended PIV issuance and maintenance processes. Further technical details in upcoming SP 800 documentation	Accept in Principle	Enrollment	Accept in Principle - The text has been updated to allow electronic iris and facial images to be used as an additional means of authentication during PIV issuance and maintenance processes.
515	Secure Technology Alliance	2 - Industry	2.7, para. 5 Line 715	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Declined	Editorial	Decline - 800-63A uses both "supervised remote proofing" and "supervised remote in-person identity proofing" interchangeably, with the latter only appearing as a single section header.
516	CISA	1 - Federal	Sec. 3, Pg. 27, Para. 1: Line 1186	Even while informative it should not be misleading. The Federal ICAM office has specified a Identity Credential and Access Management Architecture in which the PIV Card issuance, validation, and card lifecycle management can exist. Those ICAM systems are dependent on integration with the PIV Card IDMS system but the PIV Card IDMS is not sufficient for performing Federal ICAM service functions. In no cases has this commenter seen that the PIV IDMS interacts directly in the issuance of sub-accounts that are dependent on the PIV card, nor the authorizations required to use the PIV card for logical or physical access control.	Clarify how PIV Card IDMS integrates with FICAM and Agency IDMSs.	Accept in Principle	Other	Accept in Principle - The intent was not to specify a new IDMS- merely to acknowledge that the card management and issuance systems are part of the agency's broader identity management system. The updates to the text clarify these core concepts.
517	Secure Technology Alliance	2 - Industry	2.7.1 Line 778	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of issue #515

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
518	CISA	1 - Federal	Sec. Figure 3-1, Pg. 28: Line 1220	This diagram neglects to show the interposing relying system of the Agency Identity and Access Management systems which allows the PIV card to be provisioned for use on related accounts and that manages the permissions and entitlements that the account holder has upon which the PIV card or the derived PIV credential can be utilized. The PIV Relying Subsystem is substantial, and includes important not represented by the showing of the endpoints alone. Each of these PIV Relying Subsystem endpoints depend on an Agency Identity and Access Management system in order to properly maintain the accounts associated with each PIV card holder and the entitlements and privileges that are required to properly operate an Agency ICAM environment. This reliance on the ICAM architecture to carry out the mission assigned to the PIV and derived PIV responsibility needs to be clearly shown here.	Show an Agency Identity, Credential and Access Management system as a supersystem on the PIV-related systems, the PIV IDMS and the PIV Front-end Subsystems being directly connected to that system. The section that shows Logical and Physical Access is in a superposition to the PIV system as there are other means of performing both logical and physical access that do not involve the PIV system and this should be reflected in the diagram where these components are part of the larger ICAM services but that the PIV card system supports with those unique credentials	Declined	Editorial	Decline - This commentor is asking for more detail and breadth than the diagram is meant to convey.
519	Secure Technology Alliance	2 - Industry	2.7.1, para. 1 Line 779	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	duplicate	Editorial	Duplicate of issue #515
520	Secure Technology Alliance	2 - Industry	2.7.1, para. 2 Line 784	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	duplicate	Editorial	Duplicate of issue #515
521	Secure Technology Alliance	2 - Industry	2.7.1, para. 4 Line 795	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of issue #515
522	CISA	1 - Federal	Sec. 3.1.2, page 30, Para. 1: Line 1275	This statement presumes that the enterprise IDMS that is responsible for issuing a created PIV Card and the Agency Identity and Access Management systems which allows the PIV card to be provisioned for use on related accounts and that manages the permissions and entitlements that the account holder has upon which the PIV card or the derived PIV credential are one in the same. It is true that the PIV account is maintained throughout the cardholder's employment but it is not true that that account is the sole account in the Agency environment.	Clarify that account is NOT the sole account in the Agency environment.	Accept in Principle	Enrollment	Accept in Principle - The document updates clarify the PIV Identity Account term.
523	Secure Technology Alliance	2 - Industry	2.7.1, para. 4 Line 801	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of issue #515

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
524	CISA	1 - Federal	Sec. 3.1.2, page 30, Para. 1: Line 1279-1280	This is true and substantial and the ICAM-related systems needs to be shown in the diagram that sets the expectation of the systems that the PIV Card IDMS relies on. The PIV Relying Subsystem is substantial, and includes important not represented by the showing of the endpoints alone. Each of these PIV Relying Subsystem endpoints depend on an Agency Identity and Access Management system in order to properly maintain the accounts associated with each PIV card holder and the entitlements and privileges that are required to properly operate an Agency ICAM environment. This reliance on the ICAM architecture to carry out the mission assigned to the PIV and derived PIV responsibility needs to be clearly shown here.	Show an Agency Identity, Credential and Access Management system as a supersystem on the PIV-related systems, the PIV IDMS and the PIV Front-end Subsystems being directly connected to that system. The section that shows Logical and Physical Access is in a superposition to the PIV system as there are other means of performing both logical and physical access that do not involve the PIV system and this should be reflected in the diagram where these components are part of the larger ICAM services but that the PIV card system supports with those unique credentials.	Duplicate	Other	Duplicate of issue #516
525	Secure Technology Alliance	2 - Industry	2.7.1, para. 5 Line 814	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of issue #515
526	Secure Technology Alliance	2 - Industry	2.7.1, para. 5 Line 816	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of issue #515
527	CISA	1 - Federal	Sec. 3.1.3, page 30, Para. 2: Line 1294	This statement needs to be expanded in order to indicate the dependency on that Agency Identity and Access Management system to be able to determine the proper use of the PIV card for Logical and Physical Access controls which are the only entities that can provide proper authorization mechanisms. The PIV system is a subsystem of the ICAM system, and the PIV is utilized within that system to provide high-assurance identity and authentication, not the other way around.	Expand statement.	Declined	Editorial	Decline - This section describes systems from the perspective of the PIV components. There may be many other components in an overall deployment.
528	Secure Technology Alliance	2 - Industry	2.9.3, para. 1 Line 997	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of issue #515
529	Secure Technology Alliance	2 - Industry	2.9.3, para. 3 Line 1019	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of issue #515
530	CISA	1 - Federal	Sec. 5.1, page 66, Para. 1: Line 2068	Vague reference to Common Policy	Recommend providing a reference to the Federal PKI and adding it to the glossary.	Accept in Principle	PIV Card	Accept in Principle - In section 5.1 the reference to Federal PKI policy authority [PROF] is changed to reference to U.S. Federal PKI Common Policy Framework (Federal CIO Council), [COMMON]
531	Secure Technology Alliance	2 - Industry	2.9.3, para. 4 Line 1022	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of issue #515

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
532	CISA	1 - Federal	Sec. 5.5.1, page 68, Para. 2: Line 2134-2138	Is the prohibition on the HTTP protocol or the method of delivery? Is this intended to include delivery over private connections supported by HTTPS or other secure tunnels such as VPN or SSH? Is the prohibition related to publishing in public directory rather than use in authenticating to a Government system from the public portion of the Internet.	Clarify.	Duplicate	Other	Duplicate of issue #243
533	CISA	1 - Federal	Sec. 6.1, Para. 1: Line 2167-2168	Earlier you stated that the PIV did IDP requirements did not necessarily meet those of SP 800-63A but that you were utilizing compensating controls in the form of the background checks to achieve IAL3. This should be explicit here as it is VERY important in federated exchanges in that the relying party will need to understand that a compensating control is in place and not the normative guidance.	Include compensating controls.	Accept in Principle	Enrollment	Accept in Principle - A footnote was added to describe how compensating controls (in the form of federal background investigations) are used to achieve IAL3.
534	Secure Technology Alliance	2 - Industry	2.9.3, para. 4 Line 1023	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Editorial	Duplicate of Issue #515
535	Secure Technology Alliance	2 - Industry	Appendix E, p. 115 Line NA	Naming convention does not match precedent specified in NIST SP 800-63A section 5.3.3.2	Supervised Remote In-Person Proofing	Duplicate	Enrollment	Duplicate of issue #515
536	CISA	1 - Federal	Table 6-2, page 79: Line 2460	Re: BIO-A at AAL3. Since there is no way for the validation infrastructure to verify that this is a supervised event this would only be done in portions if the PIV lifecycle (issuance or reissuance), where, by policy, one could assume supervision was available because it is specified.	Recommend removing or providing an asterisk and footnote to indicate that this is a supervised operation.	Accept in Principle	Other	Accept in Principle - Table 6.2 has been revised
537	CISA	1 - Federal	Table 6-2, page 79: Line 2460	The terms “Local Workstation Environment” and “Remote/Network System Environment” need definition. PKI is an inherently “network” infrastructure. It is not possible for the Local Workstation to perform the certificate path validation specified in RFC 5280 without being able to utilize a network. This then makes the workstation a network device and not a local workstation. This then reduces the only valid AAL3 authentication to OCC-AUTH for local workstation, all the rest are network authentications.	Define terms “Local Workstation Environment” and “Remote/Network System Environment.”	Accept in Principle	Authentication	Accept in Principle - Table 6.2 has been revised with column headings updated

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
538	CISA	1 - Federal	Table 6-2, page 79: Line 2460	Re: Remote/Network System Environment AAL3 PKI-AUTH. This is the only valid category for PKI-AUTH. This Authentication is a point in time and all subsequent uses on the network are by a derivative assertion form (see Federation). For instance, once an individual authenticates with the PIV card there is generally a network assertion provided upon which all subsequent activity is performed. One is not forced to “reauthenticate” at every interaction. To do so would be a severe barrier to operations.	Delete AAL3 PKI-AUTH entry in local WS column.	Declined	Authentication	Decline - The act of authenticating to a local workstation is logging into or unlocking that workstation, not every interaction with it. As with the session secret used by an authenticated session over a network, the workstation keeps state information that determines whether it is logged in/unlocked. This shouldn't interfere with the use of PKI-AUTH.
539	CISA	1 - Federal	Sec. 7, page 80, Para. 2: Line 2464	This section severely understates the importance of assertions in the operations of computing systems. After the initial authentication (which could well involve PIV) virtually all interactions are performed through some means of assertion (either a hash function of the authenticator or a device or system-issued token) that represents the person that performed the authentication.	Recommend providing guidance on minimum security requirements for the assertion in addition to those of 800-63-3 (base and C). For example, the assertion should include attributes that make clear to the RP that the authentication was derived from a PIV authentication and who performed the authentication and when.	Declined	Authentication	Decline - More information on federation will be covered by a new federation special publication (SP800-217)
540	CISA	1 - Federal	Sec. 7.1, page 80, first sentence: Line 2469	When discussing federation protocols and the manner in which a PIV authentication can be transition to a federation assurance needs to be described (protocol transition). PIV authentication is one protocol, likely that will be transitioned into a assertion not generated by a user but generated by a system that acts on behalf of the user. This is commonly described as a delegation of authority where the system becomes the authority on behalf of the user and generates the assertion (constrained delegation). Use a diagram. It should be noted that the federation protocols are the PREDOMINATE mechanism upon which computing systems operate within a network, not as some simple aside. Consideration should be given to whether the resulting assertion should include information beyond that required in 800-63-3 (and C supplement) to inform the RP that the assertion is founded on a recent, prior PIV authentication. The information would include the identification of PIV (and holder) and the entity that performed that authentication, and the date and time of the authentication. Note that Line 2601 states that "Status of the investigation can be	When discussing federation protocols and the manner in which a PIV authentication can be transition to a federation, assurance needs to be described. Describe any additional assertion contents needed beyond that required in 800-63-3 (and C supplement) to inform the RP that the assertion is founded on a recent, prior PIV authentication.	Declined	PIV Federation	Decline - this is the purview of a federation-focused Special Publication (SP800-217). Diagram 3-3 describes the process mentioned here.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
541	CISA	1 - Federal	Line 2495	Federation protocols often support Single Sign-on (SSO) that allows a user to operate on a network without having to reauthenticate with every new action that a user takes. This frees the user from continuously entering a PIN and yet still securely perform their assigned work functions.	Add “Ease of use"	Accept in Principle	PIV Federation	Accept in Principle - The updated text will add usability benefits.
542	CISA	1 - Federal	Glossary, p 91: Line 2738	Additional explanation/description of Derived PIV Credential	Derived PIV Credential. Explain that a Derived PIV Credential has many of the cryptographic characteristics of the PIV Credential and inherits the Identity Proofing of the PIV Credential.	Declined	Derived PIV	Decline - This is in the glossary, and it's not appropriate to include a detailed description here.
543	CISA	1 - Federal	Glossary, p 91: Line 2746	FICAM missing	Add description “Federal Identity, Credentials and Access Management (FICAM)” as it is referenced as an abbreviation.	Declined	Other	Decline - FICAM is listed in Appendix C.2.
544	CISA	1 - Federal	Glossary, p 95: Line 2865	PIV credential not included	Add “Personal Identity Verification (PIV) Credential” and explain its unique characteristics as a “credential”	Accept	PIV Card	Accept - The updated document defines PIV Credential.
545	Secure Technology Alliance	2 - Industry	2.7.1, ALL Line 789-812	We suggest that section 2.7.1 of the FIPS 201-3 draft is both redundant and discordant in specifying operational parameters (e.g., see the precedent delineation of proofing requirements and guidance (i.e., local, remote, IALs, etc.) already defined in the Special Pubs Digital Identity Guidelines (NIST SP 800-63A, 800-63-3, et. al) thereby obviating the inclusion in FIPS 201-3)	The use of SRIP and requirements for SRIP SHALL adhere to the guidelines and requirements set forth in SP 800-63-3 and SP 800-63A for Supervised Remote _in-Person Proofing.	Duplicate	Enrollment	Duplicate of issue #580.
546	Secure Technology Alliance	2 - Industry	2.7.1, para. 4 Line 795-819	SRIP is simply a special use case (remote operator v. local operator) of the already established IAL3 In-Person Identity Proofing as meticulously defined in SP 800 63-3 and SP 800-63A (5.3.3.2) Supervised Remote In-Person Proofing, wherein all informative and normative compliance specifications are detailed.	Supervised Remote In-Person Proofing SHALL meet the requirements and criteria in NIST SP 800-63A.	Duplicate	Enrollment	Duplicate of issue #580
547	Secure Technology Alliance	2 - Industry	2.7.1, para. 1 Line 779	Process non-specified, implicit attribution to 800-63 undefined	…MAY use the Supervised Remote In-Person Proofing process per the guidelines specified in NIST SP 800-63A for the issuance of PIV Cards. Suggest creating a high-level section that combines items in Sect 2.7.1 line 779 - 819 and reference SP 800- 63 and 63A for specific details.	Duplicate	Enrollment	Duplicate of issue #580
548	Secure Technology Alliance	2 - Industry	2.7.1, para. 1 Line 780/781	"...issuer-controlled station, remote location, trained operator at a central location" - SP 800-63-3/2.4 allows for CSP's to be componentized and comprised of multiple independently-operated and owned business entities. Why should this not be extended to proofing? Should also align with language in 2.7.1 line 788.	…a station in a controlled-access environment that is connected to a remote location for remote operation by a trained trusted-provider. The issuer may subscribe to or contract independently for trained operator services provided they are compliant with the NIST SP 800-63A specifications and guidance for SRIP. See comment on line 25	Duplicate	Enrollment	Duplicate of issue #559 that clarified that third-parties may act on behalf of the issuer.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
549	Secure Technology Alliance	2 - Industry	2.7.1, para. 1 Line 781-783	"..goal..is to permit identity proofing in remote locations where it is not practical for them to travel.."	[blank]	Duplicate	Enrollment	Duplicate of issue #598
550	Secure Technology Alliance	2 - Industry	2.7.1, para. 2 Line 786	Should match verbiage from NIST SP 800-63A 5.3.3.2	…to achieve comparable levels of confidence and security to in-person events." The draft attribution of "closely duplicate" is superfluous and erroneous as the use of SRIP technology can enhance and improve standard in-person proofing practices.	Declined	Enrollment	Decline - SP 800-63A 5.3.3.2 does not use language such as "enhance" or "improve" in person proofing. The current text in FIPS 201 'as is' is better aligned. The goal of SRIP is to provide an equivalent level of assurance as the existing in-person proces.
551	Secure Technology Alliance	2 - Industry	2.7.1, para. 3 Line 789-794	Obviated by delineated requirements specified in NIST SP 800-63A 5.3.3.2	Contend that the draft content be deprecated as it is superseded by NIST SP 800-63A 5.3.3 describing attributes exceeding the confidence and security attained by local operators/staff. Remove from FIPS 201-3.	Duplicate	Enrollment	Duplicate of issue #580.
552	Secure Technology Alliance	2 - Industry	2.7.1, para 4 & footnote 9 Line 797	SRIP is defined as Supervised Remote Proofing in Appendix A of NIST SP 800-63-3 as – A remote identity proofing process that employs physical, technical, and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process. If the 800-63-3 definition holds, then it is discordant with the draft FIPS 140-3 language “SHALL be monitored by staff at the station location…” and footnote 9 "...where staff can see the station while performing other duties."	Supervised Remote In-Person Proofing SHALL meet the requirements and criteria in NIST SP 800-63A.	Duplicate	Enrollment	Duplicate of issue #580
553	Secure Technology Alliance	2 - Industry	2.7.1, para 4 & footnote 9 Line 797	The introduction of draft statements requiring monitoring by staff at the station location are antithesis to the benefits and intent of SRIP	If the intent is security of persons/objects, the clarification must be made to differentiate from required proofing resources (i.e., trained operators).	Duplicate	Other	Duplicate of issue #580
554	Secure Technology Alliance	2 - Industry	2.7.1, para 4 & footnote 9 Line 796/797 & footnote 9	The introduction of draft statements requiring monitoring by staff at the station location are antithesis to the benefits and intent of SRIP	What is meant by "monitored" and "staff" and for what purpose? Contend that the draft content be deprecated as it is superseded by NIST SP 800-63A 5.3.3.2 describing attributes exceeding the confidence and security attained by local operators/staff.	Duplicate	Enrollment	Duplicate of issue #580.
555	Secure Technology Alliance	2 - Industry	2.7.1, para 4 & footnote 9 Line 796/797 & footnote 9	Excludes requirements for physical security and integrity	Add "Shall employ physical tamper detection and resistance features appropriate for the environment in which it is located. " Matching the requirements in SP 800-63A.	Accept in Principle	Other	Accept in Principle - The document update elaborates on security and integrity requirements for supervised remote identity proofing
556	Secure Technology Alliance	2 - Industry	2.7.1, para 4 Line 798/799	SRIP is to be completed in complete alignment with 800-63A specifications/practices for SRIP. By explicitly stating rules within FIPS-201-3, this runs high risk of diverging from the authority and preferred specification of 800-63A for SRIP.	Strike as not applicable. This level of specification is not needed at the superior document level.	Duplicate	Enrollment	Duplicate of issue #580.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
557	Secure Technology Alliance	2 - Industry	2.7.1, para 4 & footnote 9 Line 796/797 & footnote 9	Not required by 800-63A; nor is it warranted as long as security and tamper detection is implemented	Strike as not applicable. Specification is not needed at the superior document level as full specification exists in 800-63A.	Duplicate	Enrollment	Duplicate of issue #580.
558	Secure Technology Alliance	2 - Industry	2.7.1, para 4 Line 798-799	Contrary to the notion of segmented enrollments	Language implies a single session. This is different from a segmented process. Need clarification of the language.	Declined	Enrollment	Decline - The existing language is clear that "session" does not imply that a single session needs to cover the whole proofing process.
559	Secure Technology Alliance	2 - Industry	2.7.1, all Line 778-819	The language of proofing for a PIV identity is too restrictively focused on the issuer. The PIV program itself is built for federation, upon a common chain of trust for users issued PIV Identity. Proofing processes should not be considered an integral, mandatory role of the issuer. This role can optionally be fulfilled by a trusted 3rd party	The language of proofing for a PIV identity is too restrictively focused on the issuer. The PIV program itself is built for federation, upon a common chain of trust for users issued PIV Identity. Proofing processes should not be considered an integral, mandatory role of the issuer. This role can optionally be fulfilled by a trusted 3rd party See comment above.	Accept in Principle	Enrollment	Accept in Principle - The updated document text allows outsourcing of identity proofing, issuance and maintenance processes outlined in Section 2.
560	Secure Technology Alliance	2 - Industry	2.7.1, footnote 9 Line footnote 9	Not required by 800-63A, nor is it warranted as long as video surveillance, security and tamper detection are implemented	Strike as not applicable. Specification is not needed at the superior document level as full specification already exists in 800-63A Sec 5.3.3.1 and 5.3.3.2.	Duplicate	Other	Duplicate of issue #557
561	Secure Technology Alliance	2 - Industry	2.7.1, para 5 Line 813-819	Include reference to 800-63A 5.3.3.1	"..per the criteria defined in [SP 800-76] and [SP 800-63A 5.3.3.1 and]..Sec 5.3.3.1 and 5.3.3.2.	Declined	Enrollment	Decline - Criteria are discussed and covered in the relevant sections.
562	Secure Technology Alliance	2 - Industry	3.1.1. PIV Front-End Subsystem Line 1226	The PIV Card takes the physical form of the [ISO 7816] ID-1 is incorrect.	The PIV Card takes the physical form of the [ISO 7810] ID-1	Declined	PIV Card	Decline - ISO 7816 incorporates ISO 7810.
563	Secure Technology Alliance	2 - Industry	Section 4.4.1 - 4.4.4 Contact Reader Requirements Line 2025 -2039	Contact & Contactless Requirements. These sections miss the case when a reader is not connected to a laptop or desktop that is performing certificate validation. The missing point is the PACS where readers are located throughout a site where the certificate validation system is away from the reader. This requires bi-directional communication to the back-end system such as a certificate validation system near, or inside the local PACS component. SP 800-116 R1, S Sect E2 Pg. 46. Preferably, the bidirectional communication is an industry standard such as OSDP.	Suggest adding language stating: A reader used for physical access establishes a bi-directional communication path between the card's appropriate certificate and the certificate validation system. Contact card readers SHALL conform to [ISO 7816] for the card-to-reader interface, contactless readers shall transmit the ISO 7816 commands over a ISO 14443 link to/from the card.	Declined	Other	Decline - Out-of-scope. Card-to-Reader interface is defined for all readers in section 4.4.1 and 4.4.2 as well as in SP 800-96. It is the Reader-to-host that is not defined for non-general purpose desktop computing systems. (It is defined for general purpose desktop computing systems). SP 800-96 should address OSDP if it is a candidate interface to build to.
564	Secure Technology Alliance	2 - Industry	5.5.1 Line 2134	Editorial change to allow FASC-N, UUID or both in a PIV Credential	2134 Certificates that contain either the FASC-N or card UUID in the SAN extension, …	Declined	Editorial	Decline - existing language is not exclusive.
565	Secure Technology Alliance	2 - Industry	Table 6-1 Line 2449	PAL 3 includes PKI-Authentication as an authentication mechanism to enter a PAL 3 Area. PKI-Authentication is a 2FA. To keep consistency with SP 800-116 and 116 R1, (Table 4-3, pg 15), this should be relocated to the PAL2 line.	Remove "PKI-Auth" from PAL 3 area. Add "PKI-Auth +BIO" to this area. For clarification, add Uncontrolled, Controlled, Limited and Exclusion area color codes as used in SP 800-116 R1.	Noted	Authentication	Noted - We no longer establish physical assurance levels in FIPS 201, and instead simply refer to the general assurance provided by the individual PIV authentication mechanisms. SP 800-116 will continue to be the primary reference for PACS levels. Tables in sectin 6.3 will be updated.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
566	Secure Technology Alliance	2 - Industry	Glossary of Terms, Line 2885 - 2887	Add : Conveys SOME confidence in the asserted identity's validity. Consistent with SP 800-116 and SP 800-116 R1 (Sec 5.4.1 Pg 24. A3, pg 34)	A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the card authentication key of the PIV Card and a contact or contactless reader. "Convey SOME confidence in the asserted identity's validity."	Declined	Authentication	Decline - The proposed addition is a description of the properties of the authentication mechanism, not part of its definition. As such, it is better suited for Section 6 than the glossary.
567	Secure Technology Alliance	2- Industry	Glossary of Terms Line 2889 - 2891	Add: Conveys HIGH confidence in the asserted identity validity. Consistent with SP 800-116 and SP 800-116 R1	A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV authentication key of the PIV Card and a CardHolder PIN using contact reader or a contactless card reader that supports the virtual contact interface. Conveys HIGH confidence in the asserted identity validity.	Declined	Authentication	Decline - The proposed addition is a description of the properties of the authentication mechanism, not part of its definition. As such, it is better suited for Section 6 than the glossary.
568	Secure Technology Alliance	2 _ Industry	Glossary of Terms	Suggest adding the "PKI-Auth + BIO" as a 3FA authentication mechanism. Convey VERY HIGH confidence in the asserted identity. This is a well- established 3FA authentication mechanism that is consistent with SP 800-116 and -116 R1. In addition, there are several readers on the GSA FIPS 201 EP Approved Products List. This continues to be deployed while a multitude of reader manufacturers offer competition.	In the Logical Access tables, there is no reference to this 3FA mechanism that is so important in the deployment and implementation of Physical Access Control Policies for access to the most high consequence areas. In SP 800-116 referred to as Exclusion Areas. Suggest adding the following case. A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV authentication key of the PIV Card and a CardHolder PIN using contact reader and Card Holder Biometric using contact interface. Convey VERY HIGH confidence in the asserted identity validity.	Declined	Other	Decline - The proposed addition is not in scope for FIPS 201- it is instead addressed by SP 800-116.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
569	Secure Technology Alliance	2 _ Industry	3, 3.1.3, 3.3, 6.3.1, 6.3.2: Line 1195, 1298, 1338	Derived PIV Credentials for Physical Access: OMB 19-17 states "[Federal agencies are to] develop guidance to facilitate use ... of derived credentials for logical AND PHYSICAL access". The referenced sections and page no.'s imply that a PIV card and a derived credential can be used for physical access -- for example, Section 3.1.3, Line 1298, states "The PIV relying subsystem becomes relevant when the PIV Card or derived PIV credential is used to authenticate a cardholder who is seeking access to a physical or logical resource."	1. The referenced sections imply that derived PIV credentials may be used for physical access as well as logical access, which is a good thing. If that is the intent of the draft (i.e., leaving the option open), the references should remain as is/are, and should not be modified by any comments that NIST might receive to the contrary. Some agencies are showing interest in derived credentials for physical access, and it follows that some agencies will eventually want to use mobile devices for physical access in some form within the next 2-3 years. 2. Change title of Section 6.3.1 to ""PIV Card Physical Access"". Change title of Section 6.3.2 to ""PIV Card Logical Access"". The PAL auth mechanisms are PIV-card specific, and the implication is that FIPS 201-3 is only addressing PIV physical access at this time. It would be nice to have DPC considerations for physical access in this draft, but it may be convenient be vague on it within this version, with the option that derived credentials for physical access can be addressed in other standards updates, e.g., SP 800-157. 3. This all aligns with an answer received during the FIPS 201-3 Virtual Workshop when the question was proposed -- Answer:	Accept in Principle	Derived PIV	Accept in Principle - The titles of the sections have not been changed but the following has been added to the introductory text in Section 6.3: "The authentication mechanisms described in the subsections below apply specifically to the use of PIV Cards for physical and logical access. Authentication mechanisms for physical and logical access using derived PIV credentials is described in [SP 800-157]."
570	Secure Technology Alliance	2 - Industry	General	"Relying Party", "Relying System" and "Relying Subsystem": These terms are used for what appears to be the same thing, and/or are not specifically defined or distinguished from each other.	Suggest deciding on a single term. Note that SP 800-63-3/63A/63B/63C use "relying party".	Duplicate	Other	Duplicate of issue #331

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
571	Mari Spina <mspina@mitre.org>	Self	7. Federation	The ability to find the Authoritative Federation IdP services when a user from a non-resident domain is attempting to authenticate may prove valuable in a Zero Trust Architecture. This concept is addressed by the Max.gov FedHub. The Zscaler product refers to an "IdP Redirect" (https://help.zscaler.com/zia/about-identity-providers). The Okta product addresses it as "IdP Discovery" or "IdP Routing" (https://help.okta.com/en/prod/Content/Topics/Security/Identity_Provider_Discovery.htm). Another company, WSO2, defines a "Federation Hub" (https://wso2.com/articles/2018/06/what-is-federated-identity-management/) and Mini-Orange describes the discovery process as "Domain-based redirection to ID" (https://www.miniorange.com/identity-broker-service). Years ago there was even a DHS/DoD backend attribute exchange (BAE) broker proof of concept that addressed this issue.	Suggest addition of text to allow for the use and integration of an IdP Discovery Service or a Federation Broker to handle the search, discovery, and identification of an authoritative IdPs. An IdP Broker concept is described by: https://csrc.nist.gov/CSRC/media/Projects/Attribute-Based-Access-Control/documents/july2013_workshop/july2013_abac_workshop_ksmith.pdf#page=4. Continued Rational: In a Zero Trust architecture, there may also be value in allowing multiple IdPs to provide assertions because each may hold attributes about the user that the others do not have. In the future, some IdPs may hold dynamic attributes or computed trust scores.	Declined	PIV Federation	Decline - Both discovery of "home IdP" and issues around brokers/proxies will be covered in a future PIV Federation Special Publication (SP800-217).
572	Secure Technology Alliance	2 - Industry	[blank]	Other Types of Issued Derived PIV Credential Digital Certificates: Agencies may deliver Digital Signing Certificate, Encryption Certificates and Encryption Key History Keys along with Derived Credential Authentication Certificates for derived credentials issued to mobile devices.	Agencies want to provide digital signing and encryption certs to mobile device such that emails can be signed and encrypted. Recommend reviewing and addressing these additional certificates and keys where they may apply in the draft standard, and also taking into consideration for the next version of SP 800-157.	Duplicate	Derived PIV	Duplicate of issue #332
573	Secure Technology Alliance	2 - Industry	2.2 Line 568	Continuous Vetting Program: Section 2.2 (Credentialing Requirements) states "This determination SHALL be recorded in the PIV enrollment record to reflect PIV eligibility for the PIV cardholder and, if applicable, their enrollment in the Continuous Vetting Program." Continuous Vetting Program is only mentioned once in the draft and not defined.	Recommend defining CVP, and expand on its impact/significance to Credentialing Requirements and any other relevant requirements.	Duplicate	Enrollment	Duplicate of issue # 333
574	Secure Technology Alliance	2 - Industry	2.7	Temporary Resident Card: Temporary Resident Card has been removed from the list of Forms of Identification.	Was this intentional? Did something else replace Temporary Residence Card?	Duplicate	Other	Duplicate of issue #334
575	Secure Technology Alliance	2 - Industry	5.5.2 Line 2140	Maintain the FIPS 201-2 original language here. Rational: Can be interpreted by PIV-I and CIV issuers, outside the federal government, the OCSP responder capability is supported on a "stakeholders need" basis.	OCSP [RFC2560] status responders shall be implemented as a supplementary certificate status mechanism. (emphasis added)	Declined	Other	Decline - OCSP responders were required under FIPS 201-2, and continue to be required under FIPS 201-3. Removing "supplementary" from FIPS 201-3 was intended to clarify that they are required.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
576	Secure Technology Alliance	2 - Industry	2.7 Line 739-740	Explicitly categorize non- REAL ID state IDs as acceptable for Fair evidence or that it is not usable.	ID card issued by a federal, state, or local government agency or entity, provided that it contains a photograph **to include non-REAL ID state issued driver licenses, mobile driver license, or state or jurisdictional ID card**	Duplicate	Enrollment	Duplicate of issue #376
577	Secure Technology Alliance	2 - Industry	2.7 Line 731	Explicitly recognize a state-issued mobile drive license as valid ID for enrollment for PIV	..driver's license, mobile driver's license, or state or jurisdictional ID card issued in compliance with REAL-ID requirements	Duplicate	Enrollment	Duplicate of issue # 594
578	Secure Technology Alliance	2 - Industry	2.7 Line 739	Explicitly recognize a state-issued mobile drive license as valid ID for enrollment for PIV	to include non-REAL ID, state-issued driver licenses, mobile driver license, or state or jurisdictional ID card, provided that it contains a photograph	Duplicate	Enrollment	Duplicate of issue # 594
579	Secure Technology Alliance	2 - Industry	2.7.1 Line 792	Add Logical integrity with action to be further defined in SP 800-63	ensuring that the physical and **logical** integrity of the station	Accept in Principle	Enrollment	Accept in Principle - Added new language covering malicious code threats to supervised remote identity proofing stations.
580	Secure Technology Alliance	2 - Industry	2.7.1 Line 796	This process as whole needs to better defined with controls and compensating measure. Can envision, permanent locations, mobile enrollment container, and packable suitcase type of enrollments. Recommend that physical security controls like sensors that count people into a area, cameras their views, recording resolution and frame rate of the enrollment be defined as controls. Software self check, terminal vs workstation and hardware tampering devices would be additional controls. The controls would define how the process has to be monitored. Recommend these be addressed in SP 800-63 series of publications.	Remove "SHALL be monitored by staff at the station location while it is being used." Suggest this be addressed in SP 800-63 series of documents.	Declined	Enrollment	Decline - This issue was discussed at length during the development of the the FIPS 201-3 draft. Supervised remote identity proofing stations need to be in staffed locations to protect against equipment tampering. This could be revisited in the next revision of FIPS 201. The update to SP 800-79 will provide additional clarifications regarding the responsibilities of the on-site monitoring staff.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
581	Secure Technology Alliance	2 - Industry	4.2.2.6 para. 1 Line 1900	The words “or the virtual contact interface” are missing at the end of the first sentence. According to the definition of the virtual contact interface earlier in this standard, “Any operation that MAY be performed over the contact interface of the PIV Card MAY also be performed over the virtual contact interface.” See FIPS 201-3 draft line 1814 and previous FIPS 201-2 section 4.2.2 paragraph 4. Besides both FIPS 201-2 and FIPS 201-3 draft include in section 4.2.2 Cryptographic Specifications , a sentence stating: “With the exception of the card authentication key and keys used to establish secure messaging, cryptographic private key operations SHALL be performed only through the contact interface or the virtual contact interface.“ (see FIPS 201-3 draft line 1812) Allowing the PIV card administrator to authenticate to the PIV card through a VCI enables to service the card through the NFC interface of a smart phone, for instance to reset a card when the PIV card holder is working remotely and can no longer boot his PC because his PIN is blocked. Since the card application administrative key is optional, why prevent its use for Post	Change the last sentence of this paragraph to read: If present, the cryptographic operations that use the PIV Card application administration key SHALL only be accessible using the contact interface, or the virtual contact interface, of the PIV Card."	Accept in Principle	PIV Card	Accept in Principle - Final resolution is to clarify text to indicate that Application Administration Key can only be used on contact interface
582	Secure Technology Alliance	2 - Industry	2.4 Line 594-595	This is a welcomed addition to the FIPS 201 standard, thank you! Some issuers may be tempted to use the same set of fingerprints for off-card authentication and on-card comparison simply for user convenience, without realizing the security issue such personalization could introduce. Fingerprints from OCC are freely readable from an activated card, and converting the ANSI 378 template in the card holder fingerprint data object to an ISO 19794-2 template to be used by OCC is a trivial operation. So having for on-card comparison the same set of fingerprints as for off-card authentication, results in being able to read from the card data needed to perform a card activation with OCC, and use it another time in place of PIN verification to activate the card prior to PIV Authentication or digital signature.	Keep this important addition in the final version.	Noted	Authentication	Noted - Comment confirms intent of addition.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
583	Secure Technology Alliance	2 - Industry	2.9.3, para. 2 Line 1001+D377	This paragraph is about resetting a PIV card. If the PIV card needs to be reset, that means its PIN has been blocked due to too many consecutive failed verification attempts and therefore none of the biometric data on the card can be read.	Add "through an on-card one-to-one comparison" after "PIV Card" on line 1003 in the sentence "… elicit a positive biometric verification decision when compared to biometric data records stored either on the PIV Card or in the PIV enrollment record."	Duplicate	PIV Card	Duplicate of Issue #584
584	Secure Technology Alliance	2 - Industry	2.9.3 para. 4 Line 1028	Same comment as above. This paragraph is about resetting a PIV card. If the PIV card needs to be reset, that means its PIN has been blocked due to too many consecutive failed verification attempts and therefore none of the biometric data on the card can be read.	Add "through an on-card one-to-one comparison" after "PIV Card" in the sentence "… elicit a positive biometric verification decision when compared to biometric data records stored either on the PIV Card or in the PIV enrollment record."	Accept	PIV Card	Accept - Issue #583 commented on the same issue that appeared on a different line (1001).
585	Secure Technology Alliance	2 - Industry	4.1.4.1, table 4.1 Line 1530	Examples are missing from the table; one of them is displayed in the page footer.	Fix the display of table 4.1	Duplicate	Editorial	Duplicate of #218 (part 4/5)
586	Secure Technology Alliance	2 - Industry	4.1.4.3, Zone 8B Line 1674	Depreciation of Linear 3 of 9 Bar Code. There may be a new use case for some kind of bar code in this zone on the back of the card. A bar code could be used to store the PIV Pairing Code. That would facilitate and expedite VCI establishment when readers are equipped with a low cost bar code scanner. The Pairing code would be read automatically as the card holder approaches the PIV card to the contactless PACS reader. The Pairing Code could also be encoded as a QR code or Micro QR code.	Consider converting one of the depreciated bar code zones to store a micro QR code or PDF 417 with the PIV Pairing Code.	Declined	PIV Card	Decline - SP 800-73-4 states another location for printing the pairing code (if department/agencies choose to print it). It states: The pairing code ..... may be printed on the back of the card in an agency-specific text area (Zones 9B or 10B).
587	Secure Technology Alliance	2 - Industry	4.2.2 Line 1803	The optional asymmetric private key that supports key establishment for secure messaging and card authentication for physical access is NOT the PIV Card Application Administration Key. A title is missing above this paragraph to separate from Admin key.	Add the following title above this paragraph: "Secure Messaging Key Establishment Key"	Duplicate	Authentication	Duplicate of issue #452
588	Secure Technology Alliance	2 - Industry	4.2.2.3 para. 2 Line 1869	This paragraph states that ""If used, the symmetric card authentication key MAY be imported onto the card by the issuer or be generated on the card."" It does not seem to make sense to generate on the card a symmetric key used for authentication, unless the key can be exported. Does that mean that cryptographic keys can be exported from the PIV card?	Remove "or generated on the card"	Declined	Authentication	Decline - This language was not changed from FIPS 201-2, and SYM-CAK is being deprecated as part of the FIPS 201-3 revision.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
589	Secure Technology Alliance	2 - Industry	4.3.1 Line 2010	**PIN Policy**: “The PIN SHALL be a minimum of six digits in length. The PIV Card SHALL compare the chosen PIN against a list of at least 10 commonly-chosen values (e.g., 000000, 123456) and require the choice of a different value if one of those is selected by the cardholder.” Checking the PIN format (ASCII numeric only) and the length (minimum six digits) is already performed by PIV cards since SP800-73-3 (part 2, section 2.4.3). Asking the PIV card to also filter out weak PIN values creates a significant challenge, for card manufacturers, for CMS vendors and also for Issuers. **From a Card Manufacturer’s Perspective:** To be effective, the number of so called “weak PIN values” can quickly exceed 10. Since the PIN is of variable length (6 to 8 digit) if you exclude 000000 (6 digits), you probably want to exclude also 0000000 (7 digits) and 00000000 (8 digits). And what about 111111 (6 digits), 1111111 (7 digits) and 11111111 (8 digits) and going all the way up to 99999999 (8 digits), you’ve already identified 30 weak PIN values. The second example was 123456 but if you	A: Delete the requirement starting on line 2010: "The PIV Card SHALL compare the chosen PIN against a list of at least 10 commonly-chosen values (e.g., 000000, 123456) and require the choice of a di˙erent value if one of those is selected by the cardholder." B:: Edit sentence starting at line 2008 to: “The PIV Card SHALL enforce that the PIN be a minimum of 6 digits in length. The cardholder SHOULD choose a PIN that is not easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security Number or phone number).	Accept in Principle	PIV Card	Accept in Principle - New text eliminates the need for card to check against blacklist of keys. Card Management processes will provide guidance to cardholders on PIN selection.
590	Secure Technology Alliance	2 - Industry	4.2.2.2 Line 1850, 1890	Import of asymmetric card keys. Will the [SP 800-73] be enhanced with this feature?	MAY be generated on the PIV Card by an administrator or imported to a new PIV Card by the issuer."	Noted	PIV Card	Noted - Import of the asymmetric card authentication key has been possible since FIPS 201-2 and hence in SP 800-73-4. Note - It is out of scope to specify protocol steps for import as it is a card management function.
591	Secure Technology Alliance	2 - Industry	5.2.1 Line 2100	The expiration date of the PIV authentication and card authentication certificates SHALL NOT be after the expiration date of the PIV Card. What is the origin of the expiration date of the PIV card?	Need clarification of what Expiration Date is used. Expiration date taken from the CHUID? Or the expiration date from list on a service?	Accept in Principle	PIV Card	Accept in Principle - Section 4.2.1 was updated to state that the CHUID data object is the electronic source for the card's expiration date.
592	Secure Technology Alliance	2 - Industry	[blank]	Cardholder UUID was Optional in FIPS 201-2. This is a very valuable data object and should be MANDATORY in FIPS 201-3. Also suggest changing the term to Person UUID for an intuitive term.	Make the CardHolder UUID Mandatory. Change the name to Person UUID.	Declined	Other	Decline - This was discussed in the FIPS 201-2 revision cycle and the recent FIPS 201-3 business requirements meeting, and we determined that a government-wide stable identifier was not necessary and may not be appropriate in some environments. We will, however, address stable subject identifiers for relying parties as part of the upcoming federation SP.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
593	Secure Technology Alliance	2 - Industry	6.2.3.1 Line 2264	Other card activation mechanisms, as specified in [SP 800-73], MAY be used to activate the card. Does the PIV Card support other mechanisms than specified by [SP800-73]? In what states are these mechanisms allowed?	Add specific language to show example or, include reference to specific section in SP 800-73. During initialization or personalization, other mechanism as specified …	Declined	PIV Card	Decline - OCC (of finger images) and PIN are the only mechanisms specified in SP 800-73. To add others (including other modality of OCC), it would have to be specified in SP 800-73 and SP 800-76 - so that interoperability can be maintained.
594	Secure Technology Alliance	2 - Industry	2.7 Line 731	Correcting phraseology and explicitly recognizing state issued mobile Drive's Licenses and State and jurisdictionally issued identity cards and mobile identity credentials (such as DC and US Territories) issued in accordance with Read ID requirements as valid ID for enrollment for PIV.	driver's license, mobile driver's license, or state or jurisdictionally identity credentials issued in compliance with Real-ID requirements.	Declined	Enrollment	Decline - The text has been updated with a reference to applicable DHS enforcement requirements for REAL_ID compliant credentials.
595	Secure Technology Alliance	2 - Industry	[blank]	Need for Consistency in Performing Incremental or Partial Enrollments for PIV Credential Problem: Under emergency situations, FIPS-201 issuers and security officials may be required to perform incremental or partial enrollments. This may be due to the inability for issuers to provide in-person proofing and data capture support on-local because of social distancing requirement or an applicant's inability to visit a credentialing facility. This creates inconsistencies in approaches and best practices	**Recommendation**: It is recommended that FIPS-201 provide a common baseline approach, consistent across Departments and Agencies, for applicants to receive an alternate token or Derived Alternate Credential (DAC) to employees in lieu of a Personal Identity Verification (PIV) credential that will allow personnel to gain system access to the Department and Agency networks without visiting a Credentialing Facility. See Reference DHS OCSO DAC Policies & Procedures. **Key Points:** -- It is the decision of the employee's supervisor or the contractor's program manager to determine if an applicant requires a DAC in lieu of a PIV card, then the following process must be adhered to. If a DAC is needed by a new employee or contractor -- supervisors, contract program managers, or Contracting Officer's Representatives must inform the Department or Agency Credentialing Facility. Applicants must provide a valid personal email and home address when where they can receive and sign for their pre-activated DAC and government-furnished equipment (GFE) as applicable. -- Acceptable forms of partial enrollment	Declined	Derived PIV	Decline - Alternative credentials are out of scope for FIPS 201. Per [OPM policy memo](https://www.opm.gov/policy-data-oversight/covid-19/opm-memorandum-on-boarding-processes-for-new-employees-during-the-covid-19-emergency/), agencies are able to make risk-based decisions to issue alternative credentials in certain circumstances.

Issue #	Org	Org Type	Reference	Comment	Suggested Text	Disposition	Category	NIST Comment
596	NSA Center for Cybersecurity Standards	1 - Federal	Line 941	As indicated in line 941, previously collected biometric data can be reused with a new PIV card if the expiration date of the new PIV card ins no less than 12 years after the date that the biometric data was obtained. That duration seems over-long. The Canadian Government, for example, has a 10-year validity period for their visa-related biometrics.	N/A	Declined	PIV Card	Decline - Studies show that biometrics remain matchable for >12 years, which aligns with PIV card lifecycles.
597	NSA Center for Cybersecurity Standards	1 - Federal	Line 993 and 2006	In lines 993 and 2006, it says that a maximum of 10 consecutive PIN retries may be permitted before a card is locked, unless the individual government agency requires a smaller cap. The number 10 seems excessive here. For most applications (credit card, bank account, email accounts), three is the maximum number. Unless there is a compelling reason to allow 10 tries, at most we suggest 5.	N/A	Declined	PIV Card	Decline - There does not seem to be a compelling reason to choose 5 over 10.
598	NSA Center for Cybersecurity Standards	1 - Federal	Line 1798	In line 1798, it indicates that a card may store up to 20 retired key management keys. Again, this number seems large. We would welcome answers from NIST as to why they are pushing for 20 here.	N/A	Noted	PIV Card	Noted - This is not required. FIPS 201 states that "optionally, up to 20 retired key management keys may also be stored."

Row Labels	Count of Issue #
Accept	29
Accept in Principle	68
Declined	140
Duplicate	120
Noted	29
Partially Accept	5
Grand Total	**391**