Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
1	IAB	Bob Donelson	G	Section 1	Minor edits. Change references of “computer” to “logical”	See IAB Recommended Revisions to FIPS 201
2	IAB	Bob Donelson	G	Section 1.1	Expanded, tied back to HSPD-12, combined with scope.	See IAB Recommended Revisions to FIPS 201
3	IAB	Bob Donelson	G	Section 1.2	Combined with previous section.	See IAB Recommended Revisions to FIPS 201
4	IAB	Bob Donelson	G	Section 1.3	Updated to reflect new organization.	See IAB Recommended Revisions to FIPS 201
5	IAB	Bob Donelson	G	Section 2	Expanded to reflect PIV-I compliance is mandated by Oct 2005; Tied reference to SP 800-73	See IAB Recommended Revisions to FIPS 201
6	IAB	Bob Donelson	G	Section 2.1	Augmented four HSPD-12 objectives with six functional objectives. Deleted statement specifying PIV-II content Added Use Case and Requirements • Registration • Validation • Physical Access • Logical Access Added new subsection 2.1.1 Definitions Added new subsection 2.1.2 Scope of PIV-I	This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5
7	IAB	Bob Donelson	G	Section 2.2	Replaced old process with a new one; Added a figure; Defined roles, components, identity proofing, issuance requirements and workflow.	This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
8	IAB	Bob Donelson	G	Section 2.2.1	Change title, dropped “of New Employees and Contractors” and made section apply to both new and current employees Deleted entire notion of Position Sensitivity Level Explicitly allowed centralized issuance Specified electronic aspects of enrollment package Mandated an Identity Management System (IDMS) that includes a one-to-many search for alias checking Added a detailed breakdown in additional subsections • Employer/Sponsor • PIV Application Process • PIV Enrollment Process • Identity Verification Process • Card Production, Activation, and Issuance • Suspension, Revocation and Destruction	Focus on identity and chain of trust, not trustworthiness. This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5
9	IAB	Bob Donelson	G	Section 2.2.2	This section has been changed to “Re-Issuance to Current PIV Credential Holders”	See IAB Recommended Revisions to FIPS 201
10	IAB	Bob Donelson	G	Section 2.2.3	Minor edit. Change “background” to “1:many” check.	This is consistent with identity rather than trustworthiness. See IAB Recommended Revisions to FIPS 201
11	IAB	Bob Donelson	G	Section 2.2.4	Minor edit	See IAB Recommended Revisions to FIPS 201
12	IAB	Bob Donelson	G	Section 2.3	Incorporated above in “Card Production, Activation, and Issuance”	See IAB Recommended Revisions to FIPS 201
13	IAB	Bob Donelson	G	Section 3	Section 3 and all subordinate subsections were removed. These were informative and did not add any requirements to the standard. This information may be included in a separate rationale or guidance document.	See IAB Recommended Revisions to FIPS 201

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
14	IAB	Bob Donelson	G	Section 4	Substantially reorganized and re-titled this section and subordinate subsections:	See IAB Recommended Revisions to FIPS 201
15	IAB	Bob Donelson	G	Section 4.1	Minor edits. Reformatted	See IAB Recommended Revisions to FIPS 201
16	IAB	Bob Donelson	G	Section 4.1.1	Deleted in its entirety. Procurement requirements, perhaps more appropriate for printer and inks.	See IAB Recommended Revisions to FIPS 201
17	IAB	Bob Donelson	G	Section 4.1.2	Reformatted. Added reference to expanded physical security requirements in SP 800-73	See IAB Recommended Revisions to FIPS 201
18	IAB	Bob Donelson	G	Section 4.1.3	Largely deleted. Requirements to NOT emboss, punch, or affix with decals promoted one level	See IAB Recommended Revisions to FIPS 201
19	IAB	Bob Donelson	G	Section 4.1.4	Renamed “PIV Credential Data” with 3 major subsections: • Graphical Data • ICC Data • Machine Readable Data Summarize free text in succinct table format Require that all data elements will conform to PDMF as specified in SP 800-73	See IAB Recommended Revisions to FIPS 201
20	IAB	Bob Donelson	G	Section 4.1.5	Subsumed into table above References PDMF in SP 800-73	See IAB Recommended Revisions to FIPS 201
21	IAB	Bob Donelson	G	Section 4.1.5.1	Deleted. Relegated to SP 800-73	See IAB Recommended Revisions to FIPS 201
22	IAB	Bob Donelson	G	Section 4.1.5.2	The PIV card must be activated to perform privileged operations. The PIV card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system. Cardholder authentication is described in Section 4.1.6.1 and Card Management system authentication is described in Section 4.1.6.2.	See IAB Recommended Revisions to FIPS 201

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
23	IAB	Bob Donelson	G	Section 4.1.6	Deleted. Relegated to SP 800-73 PDMF and Access Control Rules.	See IAB Recommended Revisions to FIPS 201
24	IAB	Bob Donelson	G	Section 4.1.6.1	Deleted. Relegated to SP 800-73 PDMF and Access Control Rules.	See IAB Recommended Revisions to FIPS 201
25	IAB	Bob Donelson	G	Section 4.2	Deleted. Relegated to SP 800-73 PDMF and Access Control Rules.	See IAB Recommended Revisions to FIPS 201
26	IAB	Bob Donelson	G	Section 4.2.1	Deleted. Relegated to SP 800-73 PDMF and Access Control Rules. The TIG PACS version 2.2 is a normative reference to SP 800-73 and the PDMF. Specifically. Position Sensitivity Level and Expiration Date will NOT be added	See IAB Recommended Revisions to FIPS 201
27	IAB	Bob Donelson	G	Section 4.2.2	The TIG PACS version 2.2 is a normative reference to SP 800-73 and the PDMF. Specifically. Asymmetric signature field in CHUID conforms with ICAO 9303 MRTD PKI technical guidance.	See IAB Recommended Revisions to FIPS 201
28	IAB	Bob Donelson	G	Section 4.3	Elevated to a major section. Reformatted content Removed narrative text and extracted explicit requirements.	See IAB Recommended Revisions to FIPS 201
29	IAB	Bob Donelson	G	Section 4.4	Elevated to major section Kept mandatory biometric data to be collected and retained Moved technical specifications to SP 800-73 Reorganized subordinate sections to: • Fingerprint Biometric • Facial Biometric • PIV Registration [Biometric Enrollment] and Issuance	See IAB Recommended Revisions to FIPS 201
30	IAB	Bob Donelson	G	Section 4.4.1	Minor edits. Deleted descriptive text. Specified biometric data quality, format, integrity, and confidentiality will be described in SP 800-73.	See IAB Recommended Revisions to FIPS 201

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
31	IAB	Bob Donelson	G	Section 4.4.2	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
32	IAB	Bob Donelson	G	Section 4.4.3	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
33	IAB	Bob Donelson	G	Section 4.4.4	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
34	IAB	Bob Donelson	G	Section 4.4.5	Reformatted. Added statement that no algorithmic facial recognition systems are mandatory if fingerprint is not available.	See IAB Recommended Revisions to FIPS 201
35	IAB	Bob Donelson	G	Section 4.4.5.1	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
36	IAB	Bob Donelson	G	Section 4.4.5.2	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
37	IAB	Bob Donelson	G	Section 4.4.5.3	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
38	IAB	Bob Donelson	G	Section 4.4.5.4	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
39	IAB	Bob Donelson	G	Section 4.4.5.5	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
40	IAB	Bob Donelson	G	Section 4.4.5.6	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
41	IAB	Bob Donelson	G	Section 4.4.5.7	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
42	IAB	Bob Donelson	G	Section 4.4.5.8	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
43	IAB	Bob Donelson	G	Section 4.4.6	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
44	IAB	Bob Donelson	G	Section 4.5	Elevated to major section. Reference to SP 800-73 for additional card reader specifications	See IAB Recommended Revisions to FIPS 201
45	IAB	Bob Donelson	G	Section 4.5.1	Reformatted with minor edits	See IAB Recommended Revisions to FIPS 201

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
46	IAB	Bob Donelson	G	Section 4.5.2	Reformatted with minor edits	See IAB Recommended Revisions to FIPS 201
47	IAB	Bob Donelson	G	Section 4.5.3	Deleted. Relegated to Implementation Guidance	See IAB Recommended Revisions to FIPS 201
48	IAB	Bob Donelson	G	Section 5	Deleted and all subsections are deleted. Relegated to chapter 2 and SP 800-73.	See IAB Recommended Revisions to FIPS 201
49	IAB	Bob Donelson	G	Section 5.1	Deleted and all subsections are deleted. Relegated to PIV-I, section 2 and SP 800-73.	See IAB Recommended Revisions to FIPS 201
50	IAB	Bob Donelson	G	Section 5.1.1	Deleted and all subsections are deleted. Relegated to PIV-I, section 2 and SP 800-73. Registration Database one component of the IDMS.	See IAB Recommended Revisions to FIPS 201
51	IAB	Bob Donelson	G	Section 5.1.2	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
52	IAB	Bob Donelson	G	Section 5.2	Deleted and all subsections are deleted. Moved to PIV-I, section 2 and Implementation Guidance.	See IAB Recommended Revisions to FIPS 201
53	IAB	Bob Donelson	G	Section 5.2.1.1	Moved to PIV-I, section 2.	See IAB Recommended Revisions to FIPS 201
54	IAB	Bob Donelson	G	Section 5.2.1.2	Moved to PIV-I, section 2.	See IAB Recommended Revisions to FIPS 201
55	IAB	Bob Donelson	G	Section 5.2.1.3	Moved to PIV-I, section 2.	See IAB Recommended Revisions to FIPS 201
56	IAB	Bob Donelson	G	Section 5.2.2	Moved to PIV-I, section 2.	See IAB Recommended Revisions to FIPS 201
57	IAB	Bob Donelson	G	Section 5.2.3	This and all subordinate sections have been deleted. PKI and Certificate management and policy for logical access control are within the purview of the FICC and out of scope for this document.	See IAB Recommended Revisions to FIPS 201
58	IAB	Bob Donelson	G	Section 5.2.3.1	Deleted.	See IAB Recommended Revisions to FIPS 201
59	IAB	Bob Donelson	G	Section 5.2.3.2	Deleted.	See IAB Recommended Revisions to FIPS 201

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
60	IAB	Bob Donelson	G	Section 5.2.3.3	Deleted.	See IAB Recommended Revisions to FIPS 201
61	IAB	Bob Donelson	G	Section 5.2.3.4	Deleted.	See IAB Recommended Revisions to FIPS 201
62	IAB	Bob Donelson	G	Section 5.2.3.5	Deleted.	See IAB Recommended Revisions to FIPS 201
63	IAB	Bob Donelson	G	Section 5.2.3.6	Deleted.	See IAB Recommended Revisions to FIPS 201
64	IAB	Bob Donelson	G	Section 5.2.4	Moved to PIV-I, section 2	See IAB Recommended Revisions to FIPS 201
65	IAB	Bob Donelson	G	Section 5.2.4.1	Moved to PIV-I, section 2	See IAB Recommended Revisions to FIPS 201
66	IAB	Bob Donelson	G	Section 5.2.4.2	Moved to PIV-I, section 2	See IAB Recommended Revisions to FIPS 201
67	IAB	Bob Donelson	G	Section 5.2.4.3	Deleted. Position Sensitivity Level is no longer a part of the PIV.	See IAB Recommended Revisions to FIPS 201
68	IAB	Bob Donelson	G	Section 5.2.5	Moved to PIV-I, section 2	See IAB Recommended Revisions to FIPS 201
69	IAB	Bob Donelson	G	Section 6	Content in this section was informative. It is replaced by appropriate graduated criteria, use cases, and implementation guidance per OMB	See IAB Recommended Revisions to FIPS 201
70	IAB	Bob Donelson	G	Annexes A-D	Annexes A through D provide significant guidance and are removed in favor the re-organized FIPS 201. Implementation Guidance, Certification, and Accreditation must be specified through OMB implementation and acquisition guidance.	See IAB Recommended Revisions to FIPS 201
	Detailed Comments Follow					

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change

71	IAB	Bob Donelson	G	Throughout, including
				D1, p v, par 8;
				D1, p vi, par 10;
				D1, p ix (x2)
				D1.1.2 p 2 (x2);
				D1.2.2.1 p 5 (x2), p 6 (x4);
				D1.3 p 10;
				D1.1.3.1 p 10;
				D1.3.2.1 p 11;
				D1.4.2.1 p 25 (x5);
				D1.4.4.1 p 30 (x2);
				D1.5.2.1.1 p 41 (x4), p 42 (x2);
				D1.5.2.4.3 p 47 (x3);
				D1.6.1.2 p 51;
				D1.6.1.3 p 52;
				D1.E.1 p 76 (x3), p 77
					Position Sensitivity Level (PSL). PSL measures the "trustworthiness" of a claimed identity. HSPD-12's mandate and scope is limited to establishing the claimed identity and not its trustworthiness. The two differ substantially.
					
					PSL introduces a number of issues:
					(1) the possibility that some employees with verified identity are not issued PIV cards (in apparent contradiction to HSPD-12),
					(2) it encroaches on the authority of departments and agencies to determine their own processes and procedures for determining trustworthiness and granting clearances,
					(3) it will be useful only if clearance schemes across the federal government are unified. This seems to be unlikely and out of scope
					(4) the level naming scheme of 1, 2, 3, and 4 uses names that are not meaningful or instructive.
						1. Delete all references of Position Sensitivity Level.
						2. Eliminate all trustworthiness checks
						3. Eliminate PSL field from the CHUID
						
						These changes have been incorporated in the IAB Recommended Revisions to FIPS 201

72	IAB	Bob Donelson	G	Not Present	**Graduated Criteria.** HSPD-12 mandates the inclusion of graduated criteria, from least secure to most secure. There are a number of areas where graduated criteria could effectively be specified: 1. Resistance to Tampering & Counterfeiting o Graphical o Electrical 2. Electronic Authentication o PIV Authentication o Cardholder Authentication	Add graduated criteria for each of: 1. Graphical Resistance 2. Electrical Resistance 3. PIV Authentication 4. Cardholder Authentication These changes have been incorporated in the IAB Recommended Revisions to FIPS 201, Section 7

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
73	IAB	Bob Donelson	G	D1.4.1.4, p 19-22	**Uniform PIV Appearance**. FIPS 201 PUBLIC Draft does NOT adequately specify a uniform appearance of PIVs. Recognizable, uniform appearance of PIVS across Federal issuers is needed to meet HSPD-12's mandate for "Secure and reliable" – it will allow minimally trained personnel to recognize each PIV as a Federally issued credential. To achieve a uniform appearance the following must be addressed: • Background Color and Pattern. This needs to be clearly specified, together with any allowed variations. • Zone Location and Size. Each zone must be specified to an adequate degree of precision (say hundredths of an inch.) Locations should be specified relative to a fixed reference (e.g. from top left corner) • Fonts & Font Sizes. These must need specified more tightly, especially on the front of the card. The PD merely specifies minimum size. To achieve a common look, font size variability must be limited as much as possible. Also, for a few optional fields, font type and size have been omitted entirely. • Additional Printing. A clear policy statement on what additional printing or graphics an issuer may a	Clearly and completely specify: • Background color and pattern, along with any allowed variations. • Location and size of each zone to an adequate degree of precision (hundredths of an inch.) Locations should be specified relative to a fixed reference (e.g. from top left corner) • Font sizes precisely, not merely as minimums. • Specify font type and size for optional fields that has been omitted. • Policy statement on additional printing and graphics an issuer may add. If possible, provide as an exhaustive list of what is allowed Placeholders for this information have been incorporated in the IAB Recommended Revisions to FIPS 201, Section 3.4

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
74	IAB	Bob Donelson	G	D1.4.1.2, p 17	**Uniform Graphical Security Features**. The FIPS 201 specifications for a graphical security feature – a tri-modal or bi-modal OVD or OVI are completely inadequate for providing any uniformity of this feature. Without uniformity the security features will be completely ineffective, as moderately trained individuals will have little chance of differentiating between legitimate and counterfeit PIV.	Detailed specifications for human verifiable security features must be defined and published. Forensic security features must be defined but should NOT be published in widely available public documents. (Reference how closely held the security feature specifications are for passports and printed currency) A uniform security feature should be specified outside of the FIPS 201 standard.
75	IAB	Bob Donelson	G	D1.4.1.2, p 17	**Adequate Graphical Security Features.** FIPS 201 requires only a single graphical security feature – the tri-modal or bi-modal OVD or OVI. This is inadequate protection against counterfeiting. A host of technologies are available - including holographic overlay, guilloche, very fine line, micro printing, laser engraving, laser printing, UV inks, hidden word, digital watermarking and laminate glues to name a few. To meet the HSPD-12 mandate to "be strongly resistant to … counterfeiting", much stronger specification of a uniform set of anti-counterfeiting techniques is required.	Detailed specifications for human verifiable security features must be defined and published. Forensic security features must be defined but NOT be published in widely available public documents. (Reference how closely held the security feature specifications are for passports and printed currency) An adequate set of additional security features should be specified outside of the FIPS 201 standard. The need for adequate security features has been acknowledged in the IAB Recommended Revisions to FIPS 201, Section 7.1.1.

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
76	IAB	Bob Donelson	G	D1.2.3, p 7	**Central Issuance.** 201 PUBLIC Draft does not allow central issuance: "The Issuing Authority shall photograph the Applicant at the time of Issuance and retain a file copy of the image. The identity credential shall then be personalized for the Applicant." Central issuance is more cost-effective and provides much stronger lifecycle security (in several respects, particularly from the perspective of protecting blank cardstock.)	Allow central issuance for PIV cards. This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5
77	IAB	Bob Donelson	G	Omitted Item	**Unprotected Blank Cardstock.** Unprotected blank cardstock represents the #1 vulnerability to the PIV System. Stolen cardstock enables very good counterfeits. Card production and issuance must provide for strict protections for blank cardstock – including personnel, physical, procedural, and audit security. This is particularly important at decentralized issuance sites.	Include strict protections for blank cardstock – including personnel, physical, procedural, and audit security This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5.

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
78	IAB	Bob Donelson	G	D1.4.1.6.1	**FIPS 140-2 Level 3 Operator Authentication.** Achieving Level 3 requires that PINs not be passed to the card as plaintext. The PIN will have to be scrambled in some way – such as by encrypting or hashing. This is not what GSC-IS specifies, few if any of the cards and infrastructure deployed today support this. Implementing the change, especially if providing a smooth transition period, will be expensive – likely running into $10Ms or more. Unfortunately, this change gains at best a minuscule upgrade in security. The reason is that the card can only exert control over itself, it has no control over the environment is communicating with (which must be treated as untrusted). Scrambling the PIN will provide assurance that it cannot be captured and exploited by a rogue program running on the card. But the card is already pretty well locked down, and in some cases may be totally locked down.	Delete the requirement for FIPS 140-2 Level 3 Operator Assurance. It should be an option for achieving higher security levels, but not be required in the near term. This change has been incorporated in IAB Recommended Revisions to FIPS 201. The requirement which would naturally occur in Section 4 Has been deleted.

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
79	IAB	Bob Donelson	G	D1.4.1.4 D1.4.1.5 D1.4.2 D1.4.3 D1.4.4	**Required & Optional Elements.** With the 201 PD, it is difficult to determine what data, cryptographic, and biometric elements are required and optional on the various media of the PIV card. This is because this information is spread across the document and incompletely addressed.	FIPS 201 Should explicitly define data, cryptographic, and biometric elements that are minimum and mandatory by media type: • Graphical • Contact ICC • Contactless ICC • Magnetic Stripe • Bar Code For clarity and concision, these should be presented in a table. Implementation details and all optional elements for PIV credential data must be specified by media type in the PDMF of SP 800-73. This change has been incorporated in IAB Recommended Revisions to FIPS 201, Section 3.3

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
80	IAB	Bob Donelson	G	D1.4.3, p 27, 28-29	**Restrictions on PIV Authentication Key.** From D1.4.3, the PIV Auth Key is "only available through the contact interface of the PIV card." The next sentence suggests [but fall short of explicitly stating] that PIV Auth private key operations are privileged and require activation. This is an area where 201 should allow issuers flexibility. Several departments and agencies represented in the IAB have strong requirements for physical access control. In many cases, these departments and agencies have determined that Physical access will largely occur without PIN entry. Furthermore, they wish to have the option of using the capabilities of the PIV card authenticate itself to the card reader using either the contact or contactless interface.	Clearly classify PIV Authentication Private Key operations to be non-privileged operations, so that cardholder or CMS activation is not required. All cryptographic operations are allowed across all interfaces as specified in SP 800-73 according to cross-agency interoperable use case requirements. This has been removed from the IAB Recommended Revisions to FIPS 201 and relegated to SP 800-73.

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
81	IAB	Bob Donelson	G	D1.4.4	**Restriction on Biometrics.** "The biometric data on the PIV card may only be read from an activated card through the contact interface." This is another area where 201 should allow issuers flexibility. Several departments and agencies represented in the IAB have identified strong requirements for physical access control with biometrics stored on the card used in locations where there is no PIN pad. Other departments and agencies require that biometrics be protected by PIN code and may never be transmitted across the contactless interface. 201 should accommodate both.	Delete "The biometric data on the PIV card may only be read from an activated card through the contact interface." Allow the issuer to determine which interfaces (contact, contactless, or both) the biometric may be read through and whether transmission of the biometric is a privileged operation requiring card activation. This issuer should document their determination together with the considerations and documenting the functional, usability, security, integrity, and privacy requirements. This has been removed from the IAB Recommended Revisions to FIPS 201 and relegated to SP 800-73.
82	IAB	Bob Donelson	G	Not Present	**Chain of Trust.** The chain of trust binding the cardholder, the issuer, the identity verification, the card and the biometric is not adequately presented.	Added to the IAB Recommended Revisions to FIPS 201, in Sections 2,2, 2.2.1, 2.2.1.4, and 7.2