Subject: DRAFT FOR SUBMITTAL: " Comments on Public Draft FIPS 201"
From: "Bruce Mahone" <bruce.mahone@aia-aerospace.org>
To: <DraftFips201@nist.gov>

SUBJECT: Submittal of Comments on FIPS 201

On behalf of our member companies, the Aerospace Industries Association is pleased to submit the attached Comments on Public Draft FIPS 201 for your evaluation. The comments are the result of a thorough review of the Draft FIPS 201 by security experts in major aerospace manufacturers. We hope that you will find the comments and suggestions of value in finalizing the standard.

We appreciate the opportunity of participating in the development of the Personal Identity Verification (PIV) Standard.

Sincerely,

B. Mahone
(Submitter)

Bruce L. Mahone
Assistant Vice President
Technical Operations
Aerospace Industries Association
1000 Wilson Blvd, Suite 1700
Arlington, VA 22209
Phone: 703-358-1095
Fax: 703-358-1195
Mobile: 703-568-0766


FIPS 201 Comments-AIA.xls

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
1	Aerospace Industries Association (AIA)	Mr. Bruce Mahone, (AIA) Assistant VP, Technical Operations	T	[PROF] Many references	PROF refers only to the PKIX IETF activities. The PKInit specifications of the Kerberos Working Group, though still in draft form are extremely important and are already in widespread deployment in some Federal (particularly DoD) agencies. Special profile requirements to support PKInit are extremely important.	
2			E	1.2 Scope., Page 1	"Federally-controlled information system", should be plural	"Federally-controlled information systems"
3			G	2.1 Control Objectives, Page 4	Meaning is unclear in the first sentence of the last paragraph. Is the intent to state that identity proofing and issuance standards are maintained in PIV-II, and that PIV-II requires the use of a common Government-wide, interoperable PIV card? If so, the sentence needs to be reworded. As it stands now, the sentence appears to indicate that the requirements for identity proofing and issuance are maintained in PIV-II, but that the requirement for a common Government-wide, interoperable PIV card is not part of PIV-II.	PIV-II establishes and maintains these identity proofing and issuing requirements, including the requirement of a common Government-wide, interoperable PIV card.
4			T	2.2.1 page 5	The language used makes this section a little difficult to follow at first.	Differentiate more clearly between the applicant's chain of events and the requesting/authorizing official's chain. A flowchart would likely be helpful here given the criticality of this piece of information. An idea of which events could happen in serial or parallel would also add clarity
5			T	2.2.1 page 5	Reference is made to photocopies and signatures - all of which would indicate reliance on a paper based process	Include wording that would allow for scanned copies of the documents to be stored electronically at the RA as well as the digital signature of authorization forms.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
6			G	2.2.1 Page 5, paragraph 2, second sentence.	Sentence states the applicant provides the two forms of identification to the PIV Registration Authority. However, in the paragraph following Table 2.1 it states the applicant will appear in person and provide source documents provided earlier to the PIV Requesting Official. No mention is made of when this original presentation to the PIV Requesting Official was made. Not sure if the first paragraph should state the applicant provide these documents to the PIV Requesting Official, or if these is simply a step missing.	Need to better depict the chain of events... 1. applicant presents documents to PIV Requesting Official, 2. PIV Requesting Official submits forms and photocopies of identification documents to the PIV Authorizing Official, 3. PIV Authorizing Official approves and sends approved forms and photocopies of identification documents to PIV Registration Authority and the PIV Issuing Authority, 4. The applicant appears in person before the PIV Registration Authority, presenting the same identification documents as were originally presented to the PIV Requesting Official, 5. The PIV Registration Authority verifies the person matches the documents presented, and that they match the documents approved, fingerprints the applicant, performs the necessary background checks, and if successful, notifies the PIV Issuing Authority that an identity credential can be issued to the applicant.
7			T	2.2.1 page 6	Will the fingerprint information be checked against a known felons list with any sort of regularity?	Additional language regarding fingerprint usage
8			T	2.2.1, page 5	The first sentence states that "paper-based documents by themselves provide very weak assurance of identity." However, supplementing the process with background chaecks does not necessarily improve the identity assuarnce since you are using the weak paper based	
9			T	2.2.1, page 5	In the second paragraph you begin to describe the workflow for identity vetting and proofing. Step 1 is the applicant provides 2 forms of ID to the PIV *RA*. The next step indicates that the PIV *RO* submits the request and copies of the identity source documents to the PIV *AO*. There seems to be a step missing where the RA provides the documents to the *RO*. Please clarify the the interaction between the *RA* and the *RO* at the start of this process.	
10			T	2.2.1, page 5	There does not seem to be any requirement for the transfer of docuemnts to be transferred between AR, RO, RA, IA and the applicant digitally. If a digital transfer were done what are the requirements for digitallly signing the documents?	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
11			G	2.2.1, page 5	The vetting process may take quite a long time depending on the sensitivity level of the position and the type of background investigation required. What are organization required to do with employees as they await the results of the investigations. Giving them temporary badges seems like it defeats the purpose of HSPD-12 since it could give an unwanted individual exposure to areas, data, systems etc. that they should not have.	Need to add requirements for how agencies handle employees who are waiting for investigations to complete.
12			E	2.2.1, Page 5	last sentence on page "...background information listed Table 2-1." is missing a word.	...background information listed in Table 2-1.
13			E	2.2.3, page 7		Change "long-tem" to long-term"
14			G	2.3 Page 8	The list of items maintained by the issuing Authority, includes insufficient information to allow the PIV Issuing Authority to tie the PIV credential back to the PIV identity credential holder. All that appears to be required is the name of the applicant, which will result in many collisions.	If there is no need to tie the identity credential back to the identity credential holder, for instance, in the case of a lost card, how does PIV Issuing Authority know which Joe Smith identity credential to revoke? It would appear a better cross reference requirement would be established, either in the form of requiring the PIV Issuing Authority to keep sufficient identity credential holder information to make this proper identification or in the form of the PIV Issuing Authority supplying the identity credential serial number back to the PIV Registration Authority for inclusion in their maintained records.
15			T	2.3, page 7	The last sentence of the first paragraph states that the "identity credential shall then be personalized for the Applicant." What does personalize mean at this stage? Is it simply printing out the badge with the picture and other text information on it or does it also include the storage of the digital certificates, facial image, fingerprisnts and other data with the smart chip?	
16			E	3.2, Page 11	"All entities..... play a critical role"	"...all entities.....play critical roles" or "...each entity.....plays a critical role"
17			E	3.2.1, Page 11	Second bullet should be modified to reflect current common terminology usage.	"Proofing and vetting Applicants for PIV cards;"
18			G	3.2.3, page 12	The second bullet implies that PIV systems are only applicable to the Federal Government and not industry. Please clarify the impacts to industry? Are corporations that do contract work for the Federal Governement expected to be able to interoperate with PIV systems?	
19			G	3.2.3, page 12	Will contractors be expected to or allowed to access the federal system to verify the identity of a visiting federal employee?	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
20			E	3.2.3, Page 12	Fourth bullet should be modified to reflect current common terminology usage.	"OPM is responsible for assisting agencies in proofing and vetting of applicants in accordance with relevant laws and executive orders."
21			E	3.3.1, Page 14	Paragraph 3. Data is either singular or plural. Verbs in second sentence need to agree.	"the data...include...and are..." or "the data...includes...and is..."
22			E	3.3.1, Page 14	Paragraph 4. "...biometric reader may be located at secure locations..."	"...biometric readers may be located at secure locations..."
23			E	3.3.1, Page 14	Paragraph 5. "... a PIN pad device...along with the card readers..."	"... PIN pad devices...along with the card readers..."
24			E	3.3.2 Page 15	Sentence two: subject verb disagreement...	"This Key Management component is used..."
25			E	3.3.2, page 14	First sentence	Change "Figure 3-1 refers to process" to "Figure 3-1 refers to the process"
26			E	3.3.2, Page 15	First sentence - The wording is confusing...should it be that the applications are able to prohibit the use of certificates that are no longer valid? Or is it that the applications are prohibited from using the certificates that are no longer valid? Or is it something else entirely?	Specify the intent of the statement more clearly. Suggested: "...certificates so that applications can prohibit the use of certificates which are no longer valid, are all part of the Key Management component."
27			T	3.3.3. page 15	Logical resources mentioned are network locations such as computer workstations, folders, files, database records or software programs. Is netowrk access using smart card authentication or authentication to the network not included?	
28			E	3.3.4, Page 16	The PIV card usage explanation is hard to read and implies that the cardholder is providing the physical or logical access.	PIV card usage -- The main purpose of issuing a PIV card is to allow cardholder authentication or verification at a later point in time, prior to providing the cardholder the physical or logical access. Access authorization decisions can be made after successful cardholder authentication.
29			E	3.3.4, Page 16	The PIV card maintenance explanation is hard to read.	PIV card maintenance -- This activity deals with the maintenance or update of the physical card and the data stored thereon. Such data includes various card applications, PIN, PKI credentials, and biometrics.
30			E	3.3.4, Page 16	The PIV card termination explanation is hard to read.	PIV card termination -- The termination process is used to permanently destroy or invalidate the PIV card and all included data and keys so as to prevent any future use of the card and credentials.
31			E	4, Page 17	Last sentence - second paragraph -- subject - verb mismatch. "Formats....is defined..."	"Formats...are defined..." or "Format...is defined..."
32			E	4.1, Page 17	First sentence -- subject - verb mismatch. "Sections....provides..."	"Sections....provide..."

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
33			G	4.1.3g Page 18	Does the requirement indicate that a hole a the top of the card to allow attachment of the card to a clip is not allowed?	Need to specify the placement of the hole punched in card to allow attaching card to a clip.
34			G	4.1.4.1.a , Page 19	Last sentence states optional photo border -- if its optional, it can't be mandatory, and should be omitted from the mandatory information section.	Remove last sentence.
35			E	4.1.4.2.b, Page 21	Second sentence contains extra words/characters. "...consisting of s of six characters..."	"...consisting of six characters..."
36			E	4.1.4.3.d, Page 22	First sentence missing words "A bar code may be placed left side..."	"A bar code may be placed on the left side..."
37			G	4.1.6.1, Page 24	Paragraph 2. Sentence 4. Sentence is poorly worded -- implies the only time this mechanism shall be used is in the event of loss or theft. In fact, the mechanism should work regardless of the reason. An authorized cardholder who cannot remember his PIN should be prevented from gaining access.	"The PIV card shall include mechanisms to limit the number of invalid PIN attempts, as a safeguard against unauthorized access by holders of lost or stolen cards."
38			E	4.1.6.1, Page 24	Paragraph 3. Sentence 2. Comma is in the wrong place, rendering the sentence meaningless. "...transmitted to the PIV card, and ..."	"...transmitted to the PIV card and, ..."
39			E	4.1.6.1, Page 24	Paragraph 4. Sentence 2.Hyphen missing.	"in-house"
40			G	4.1.6.1,Page 24	Meaning is unclear. First sentence states that every card shall implement PIN-based cardholder activation. However, it then states that optionally PIV cardes may implement biometric activation. Is this in addition to the required PIN activation?	"Every PIV card shall implement cardholder activation by either PIN or biometrics."
41			E	4.2.2, Page 26	Paragraph 1. Sentence 2. Verb tenses don't match.	"[PACS] specifies a tag ..., but does not specify" or "[PACS] specified a tag..., but did not specify..."
42			E	4.2.2, Page 26	List under table. Poor choice of words for sentence.	"The CMS external digital signature must comply with the following requirements:"
43			E	4.3, Page 27	First sentence –missing phrase.	Should add "and is optional " to the end of the sentence.
44			E	4.4, page 30	In the second paragraph, add the word "the" before "primary"	Change "Fingerprints shall be primary biometric" to "Fingerprints shall be the primary biometric"
45			E	4.4.3, Page 32	Paragraph 5. "These images...represent the left four fingers...right four finger..."	Should be "These images...represent the left four fingers...right four fingers..."
46			E	4.4.3, Page 32	Paragraph 6. "..where each pixel represented by..."	Should be "...where each pixel is represented by..."

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
47			E	4.4.3, Page 32	Paragraph 7. Sentence 2. Subject-verb disagree. Hard to read.	Should be "Alternate compression algorithms, such as JPEG 2000, are not recommended as their standards specify several versions/options and there exist no baseline versions." or "The alternate compression algorithm, JPEG 2000, is not recommended as its standard specifies several versions/options and there exists no baseline JPEG 2000 version."
48			E	4.4.4, Page 34	Paragraph 1. Sentence 4. Extra word.	Should be "At the authentication station…left index finger and (b) an impression…"
49			E	4.4.5.1, Page 35	Sentence 4. "center's" should be "center" or "centers"	Should be "Particularly the center of the subject's…" or "Particularly the centers of the subject's…"
50			E	4.4.5.5, Page 35	Sentence 1. "trade off" should be "trade-off"	Should be "trade-off"
51			E	4.4.5.8, Page 37	Sentence 2. Confusing sentence.	"A quality measuring implementation, for which a certification and calibration may be required, should produce a value on the range 1 to 100 which shall be used and interpreted as follows:
52			E	4.4.6, Page 38	The CMS external digital signature must contain the following elements:" is misleading, since it specifies thing that should NOT be contained.	"The CMS external digital signature must comply with the following requirements:"
53			T	5.1.2 page 40	The last sentence of the 3rd paragraph states that the CA's issuing certificates for PIVs must host an LDAP for its CRL as well as any cross-certificates required to construct a path to the federal bridge. This is the first time the FBCA is mentioned in this document. Is it safe to assume that certificates issued by CAs that issue authentication certificates at FBCA medium level assurance or higher would be acceptable as authentication certificates for PIVs?	Please define what FBCA assurance level authentication and to a lesser extent encryption certificates need to comply with to be acceptable for use as PIV certificates
54			T	5.1.2, page 40	In the secoind paragraph, it states that the "lifetime of authentication certificates is long, typically several years". It also states that the expiration date of the authentication certificate shall not be after the expiration of the PIV card however no requirement is defined for the validity period for a PIV card or certificate. Please clarify the requirements for validity periods.	
55			T	5.1.2, page 40	The 4th paragraph states that "every CA that issues PIV authentication certificates shall operate an OCSP server." This implies that every OCSP agents need to be installed on all servers and desktops that use the PIV authentication certificate. How is the Federal gov't prepared to support the distribution of the OCSP agent to consuming applications?	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
56			E	5.1.2, Page 40	Paragraph 2. Sentence 3. "...(and it's associated..)..." is incorrect.	"...(and its associated..)..."
57			G	5.2.1 page 40	A CA provider - either commercial or government could take a significant amount of time to turn around an approval for a PIV. Alternatively, the PIV RO could take a significant amount of time to submit the paperwork and hold up the process this way. This could lead to a contractor/employee in limbo or worse - a temporary badge might be issued that would undermine the security of the whole system. A firm rule in IT is a system that isn't user friendly or does not meet the business needs of the organization will be discarded or avoided.	Maximum time frames for non-exception applications should be imposed on the PIV applicant, PIV RO, PIV AO and Issuing Authority for their respective activities.
58			T	5.2.1, page 41	At the bottom of the page you state that the RA "may optionally also photograph the applicant for personalization of the card." I thought that the photograph and the resulting facial image were required?	
59			E	5.2.1., Page 41	Format of requirements is inconsistant	Properly bullet separate requirements, and end each requirement with the applicable punctuation.
60			E	5.2.1.1, page 40	Sentence should be modified for consistency of terminology usage.	"An Applicant applies for an identity credential as a part of the proofing process for Federal employment."
61			E	5.2.1.2 page 42		The word "expect" should be "except"
62			E	5.2.1.2, Page 42	Wrong word.	"expect" should be "except".
63			E	5.2.3.1, Page 42	Certificate Authority should be plural.	"Certificate Authoritites (CAs)"
64			T	5.2.3.2 page 43	The COMMON policy is referenced multiple times. What is not clear is the minimum assurance level the PIV certificates must conform to. There is no clear mapping between DOD, FBCA, and now this FIPS for assurance levels. Hardware storage is obviously a given	A single set of assurance levels are required to make this interopérable (I would strongly urge the FBCA model). Further a minimum assurance level with specific proofing/vetting extensions would take care of the whole issue. I would recommend the FBCA medium level of assurance as the minimum given both the relatively close mapping (proofing, 18 hr. CRL publication, etc.) to this FIPS's requirements as well as the body of work and agreements already in place around medium level assurance.
65			T	5.2.3.4, page 45	The specification requries LDAP distribution of CA certs and CRL's. Why is HTTP distribution not included?	
66			E	5.2.4.2, Page 46	Paragraph 2. Indicates the reissuance process must be used for expired PIV cards. 5.2.4.1 indicates the renewal process is followed for expired PIV cards. Since the two processes are not the same, which is the correct process to follow for expired PIV cards?	Remove "expired cards" from first sentence of second paragraph.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
67			E	5.2.5, Page 47	Sentence 1 is poorly written, making it hard to read.	"The termination process is used to permanently destroy or invalidate the usage of the card and the data included thereon, including the keys, such that it cannot be used again."
68			E	6.1 page 49		"supported" and "PIN" are together and should be seperated by a period and two spaces.
69			E	6.1, Page 49	Paragraph 2, sentence 1 is redundant with the statement in Paragraph 1 sentence 2.	Combine sentence 1 and 2 to read, "In environments where PIV readers are available, electronic authentication of the cardholder may be conducted using the PIV card."
70			E	6.1, Page 49	Paragraph 2, sentence 5 appears to be two sentences, missing the punctuation.	Break sentence 5 into two sentences to read, "For privacy reasons, contactless use of PINs and biometrics is not supported. PINs and biometrics may be used with the PIV card using contact readers."
71			T	6.1.3, page 52	Why is the check of the expiration date of the CHUID optional?	
72			E	6.1.3, Page 52	3) Sentence is poorly written.	3) "The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source."
73			E	6.1.4, Page 52	Sentence 2 is missing a word. "...stored a PIV..."	"...is stored as a PIV..."
74			E	6.1.4, Page 53	3) word missing "...to the card requests..."	"...to the card and requests..."
75			E	A.2.1, Page 60	Sentence 3. extra space "...pre- validated..."	"...pre-validated..."
76			E	A.2.1, Page 61	Paragraph following Table A-4. Sentence 1. Uses the word "both" and then specifies three items.	"(...hardware, software and firmware)"
77			E	E.1, Page 73	Credential - wording is incorrect - subject/verb disagree.	"Credential: An object, controlled by an individual, which authoritatively binds an identity (and, optionally, additional attributes) to that individual."
78			G	Figure 3-1 page 13 - Section 3.3.3 Page 15	It seems reasonable to assume that not all facility doors will be equipped with a fingerprint reader. What does the policy say about minimal information that must be verified about the PIV card holder at access time? The last sentence of Section 3.3.3 seems to suggest that the biometric (I think it's possible to infer that this is both fingerprint and face) is the only optional piece during an access event.	A clear description of the minimal information to be captured at vetting/application has been specified. This has not been specified about information to be verified at the time of access. A definition of minimal would be desirable.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
79			G	Figure 3-1, Page 13	The importance and scope of directory services are not adequately depicted in this functional diagram. Directories are not typically dedicated to sub-functions such as PKI, but rather provide all support functions for some scope of systems. A common directory service that supports Identity and Access Management, among other uses, would also need to support PKI to integrate PKI mechanisms to all other I&AM functions. This is a fundamental concept moving forward and critical to the long-term success of PIV and PKI programs.	
80			E	Section 1, page 1		In the second paragraph change "is" to "are".
81			G	Section 1.2, page 1	States that HSPD-12 establishes requirements for common identification for Federal employees and contractors (including contractor employees). What is the difference between contractors and contractor employees and how do you define what a contractor is?	
82			G	Section 1.2, page 1	States that HSPD-12 establishes requirements for common identification for Federal employees and contractors (including contractor employees). Is there a distinction between a contractor who provides employees to work fulltime on a government site vs a contractor whose employees must visit government sites at times?	
83			G	Section 2, page 4, Common Identification and Security Requirements	In the first paragraph, you state that this section provides requirements for the identity proffing for new employees. Further in the section you mention the identity proofing concept also applies to re-issuing identity credentials for current emplyees. In this case is the identity credential that you discuss the PIV card or is it simply a renewal of a digital certificate? If it is the renewal of an authentication credential does this imply that to get the new authentication credential a current employee would need to wait for the background checks to complete to continue doing the job he has been doing?	
84			G	Section 2, page 4, Common Identification and Security Requirements	I think the real question here is will the current employee be allowed to continue in their current position while the new identity proofing process is conducted and what actions will be taken in the event that a current employee is found to have an unacceptable background?	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
85			G	Section 6, Page V	This section states that the standard is applcable to "identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees)...". I am looking for clarification that this statement implies that this does not impact the way that organizations that do business with the Federal Government have to meet the standard.	
86			G	Section 6, Page V	This section states that the standard is applcable to "identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees)...". Does this imply that contrators doing business with the Federal Governemnt have to meet this same standard for their employees who may be visiting a government facility?	
87			G	Table 2.1, page 6	How do the sensitivity levels relate back to NIST 800-63, or the DoD Levels of Assurance? If an agency complies with this standard, at what level of assurance, based on either NIST 800-63 or the DoD criteria, can be assured by the identiy proffing an vetting process?	
88			G		This document seems to mix process and technology. I don't believe that a standard should define the technology that needs to be implemented but should define what needs to be accomplished and what standards need to be adhered to.	
89			G		How does a program like DCIS-FICS fit into this or the DoD IECA/ECA program.	
90			G		How does this impact large corporations that do business with the Federal Government? I assume that the standard does not apply to identities issued by those corporations even though they do large amounts of business with the Government.	
91			G		If a large corporation were to meet the requirements of the specification, would there corporat badges be acceptable for access to Federal facilities and information resources?	

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
92			T	2.2.1, Page 5	Submission of identity documents relies solely on a paper process. This causes two types of problmes. First, there are procedural issues related to paper processes. These include: longer workflow, inability to automate the process, and inability to batch process organizational or other groupings of applicants. /In addition, an increasing number of these documents are hard copies of information and forms from digital originals. The second type of issues are security related. These include: reliance on photocopies (which are easier to forge than originals), potential for leakage of documents anywhere in the process flow which could pose security or privacy risks, and the inability to securely archive copies for future reference.	Suggest allowing, as an option, the ability for the PIV Requesting Official to digitally sign and encrypt digital copies of the identity source documents.
93			G	2.2.1, Page 5	During the transition to the PIV Credential will existing, legacy credentials (which I assume would become invalid at some point in time) be acceptable as identification source documents. That is, will PIV proofing be done from scratch or rely on these existing credentials?	
94			T	2.2.1, Page 6	It seems odd that a current photograph of the applicant is taken on identity credential issuance (2.3); but not on application (2.2.1). In addition to providing a record of the match between the applicant and the photos in the identity source documents it would be useful for checking against criminal/terrorist databases.	
95			E	2.2.1, page7		Shouldn't the bulleted list explicitly include fingerprints?
96			E	2.3, page7-8		Shouldn't the bulleted list explicitly include applicants photograph?
97			E	4.1.4 Figure 4-1, page 19	Inconstantcy between optional designation on illustration and text description.	Mark Zone 10 and Zone 11 as optional in Figure 4-1
98			T	4.1.5, Page 23	Although there is provision for optional logical credentials, no mention of an asymmetric key pair for encryption is made. It it intended that the PIV card not support encryption and if so will the DoD retain CAC cards in addition to PIV cards?	
99			T	4.4.1, Page 31	How do authentication devices used in subsequent authentication attempts know which two fingerprints are on the card? How would the PIV Card user know which ones to place on the sensor during authentication?	
100			T	4.4.1, Page 31	Is the recommendation for biometric verification during card issuance a requirement or just a suggestion?	Suggest that this either be a requirement or not.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
101			T	4.4.4, Page 34	This seems to answer #8 above as long as the applicant has readable prints on both index fingers - I still wonder if there is a provision for alternate fingers and any way the card can let the authentication mechanism know this.	
102			E	5.2.1, Pages 41-42		Suggest using "PIV Registration Authority" where "Registration Authority" is used to match roles defined in Section 2 and avoid confusion with PKI Registration Authority which might result from PKI discussion in prior subsection.
103			E	5.2.4.3, Page 47	Is there a similar process for downgrading a sensitivity level?	
104			G		If a contractor's badges met the PIV Card requirements is there any provision for reciprocity for either physical or logical access?	
105			G	2.2	Depending on the delegation of roles as defined in section 2.2 this may or may not place additional technological burden on companies. For example, if the government will delegate the roles to the extent that we would become a "registration" or "issuing" authority, this may require companies to incur costs to procure the necessary technology to meet those requirements.	
106			G		Affirmation of FIPS46-3, which specifies Triple DES as an encryption standard, is supposed to be completed every 5 years. The last affirmation was done in 1999, but Triple DES is still specified in FIPS PUB 201. Is this to assume that FIPS46-3 is to be re-affirmed now, and at the next affirmation intervals between now and 2010?	
107			G		The specification of increasing key-length requirements as time progresses is a good one, but isn't this planned obsolescence? Why not simply implement the strongest intended key-length immediately? Starting low and then moving over time may require the replacement of hardware or software at future dates to accommodate the increase, whereas if specified now, replacement would not be required.	
108			G	4.4.2 through 4.4.4	Section 4.4.2 through 4.4.4 specify fingerprint requirements for authentication. No consideration is given to users with a disability that may prevent fingerprint enrollment, such as a bilateral hand amputee.	
109			G		There are several mentions of tamper-proofing as related to the PIV card, but no mention of tamper-proofing for the PIV card reader equipment.	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Cmt #	Organization -	Point of Contact:	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
110			G		Use of Secure LDAP (S-LDAP) should be specified as compared to simple LDAP to enforce encryption of key-exchange between components. Without this, a man-in-the-middle attack whereby a compromised key is substituted for the requested key may be possible.	

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical