Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
			G		Recommend that ISO/IEC 7816-11 standard be mandated for storage of data on PIV cards. Adherence to this standard will aid in system interoperability.
	Booz Allen Hamilton		G	Section 2.2, throughout	A standard on Identity Verification should not be concerned with the "sensitivity" of a person's job. The attribute "Position Sensitivity Level" would be used in an access control decision function. The characteristic that is important to establishing identity is the level of rigor that was used in initially (at registration) verifying the identity of a person. The levels and checks listed in Table 2-2 are acceptable if the first column is relabeled something like "registration assurance level". The definition of those levels should follow: OMB 04-04 E-Authentication Guidance for Federal Agencies. Agencies may have different Position Sensitivity Levels that require that the people that fill those positions need to carry a token that asserts their identity based on a certain Registration Assurance Level (because the applications or facilities that they access will make an access control decision based on proving their identity with a certain level of assurance). If an Agency is making an access control decision based only on Position Sensitivity Level, it does not need a Perso
	Booz Allen Hamilton			Section 3.2.1, p.11	The first and last bullet relate to privilege based access control
	Booz Allen Hamilton		T	Section 3.3.1 pg 14	When are additional layers of assurance required? ie. Biometrics, key pad. What are the levels of assurance and required levels of protection?

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
	Booz Allen Hamilton		T	Section 3.3.2 pg 14	It is not clear as to how sysmetric or private keys of an asymetric key pair are delivered.
	Booz Allen Hamilton		T	Section 4.1.5.1, first set of bullets, p.23	Specify what type of biometric data is being saved on the card (images or templates). Use of the word "biometric" is redundant.
	Booz Allen Hamilton		T	Section 4.1.6 pg 24	Interoperability concerns - (Allowing the option for biometric vs. key pad). For those agencies that choose biometrics to enhance security, is the PIN/key pad as an alternative access mechanism acceptable (if the biometric fails).
	Booz Allen Hamilton		T	Section 4.1.6.2 pg 24	"If supported, card management keys shall meet the minimum algorithm and key size requirements stated in Table 4.1." This statement sounds as if card management keys that do not support the algorithm and key size requirements will be allowed.
	Booz Allen Hamilton		E	Section 4.2.2, p.26	The reference [CMS] is not listed in Annex F
	Booz Allen Hamilton		T	Section 4.3 pg 27	"As above, useful optional functions include key pair generation and trust anchor storage." While the use of the functions may be optional, it should be a requirement to have the capability."
	Booz Allen Hamilton		T	Section 4.3 pg 27	While exportation of X.509 certificates is not listed as a capability, it is important to note that the feature should not be allowed.
	Booz Allen Hamilton		E	Section 4.3 pg 29	Section reference for Activation by Card Management System not listed.

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
	Booz Allen Hamilton		T	Section 4.4	While it is recognized that, for interoperability purposes, specific biometric modalities (fingerprint, face) must be specified, this specification should allow for the use of other/additional modalities.
	Booz Allen Hamilton		T	Section 4.4, p.34, 1st paragraph	This section says "At the authentication station, two fingerprints shall be captured...". Does this really mean to imply that every application that uses fingerprints for authentication MUST capture BOTH index fingers and verify them? Does verification require that both verify or that one of the two verifies (AND vs. OR)?
	Booz Allen Hamilton		E	Section 4.4.6, p.37	The reference [RFC 3852] is not listed in Annex F
	Booz Allen Hamilton		T	Section 4.4.6, p.37	If the intention here is to define a CBEFF compliant Patron Format then there needs to be more definition of the construction and encoding of the Patron Format (including the registration of a CBEFF Patron Identifier). If the intention is to define a CMS signature that is generated on certain pieces of another data element (the CBEFF formatted biometric data) then there needs to be more definition on how those pieces are extracted from the full data element (e.g., some Patron Formats have type and length fields - are they included in the signature?) to create encapContentInfo.
	Booz Allen Hamilton		T	Section 4.4.6, p.37	If multiple CBEFF Patron Formats are possible, there must be an identifier someplace on the card to indicate which Patron Format is present (The CBEFF specification does not include a Patron Format identifier).

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
	Booz Allen Hamilton		T	Section 4.4.6, p.38, in SignerInfo and last paragraph	Unsure of the use of the term "authenticated attributes". RFC 3852 includes the type "SignedAttributes" in the Signed-data Content Type. An Authenticated-data Content Type is a different content type than a Signed-data Content Type
	Booz Allen Hamilton		T	Section 4.4.6, p.38, in SignerInfo	Needs to include an element to specify the digest algorithm (as in 4.2.2).
	Booz Allen Hamilton		T	Section 4.4.6 and Section 4.2.2	Both sections define the generation of digital signatures. One refers to CMS and the other to RFC 3852.
	Booz Allen Hamilton		T	Section 4.4.6 and Section 4.2.2	Since the PIV supports both RSA and ECDSA signatures, SignerInfo must include SignatureAlgorithmIdentifier.
	Booz Allen Hamilton		T	Section 5.2.1.1, last sentence on page 41	Says "The Registration Authority may optionally also photograph the Applicant...". Section 4.4 says an electronic facial image "SHALL be collected and used". Is the storage of a facial image on the card mandatory?
	Booz Allen Hamilton		T	Section 5.2.2.3 pg 45	Provide clarification as to whether or not 18 hour update time for CRL and OCSP is how often the CRL is updated or the how often the end user's client is updated with the CRL (next update time).
	Booz Allen Hamilton		T	5.2.4.1 pg 46	Last sentence indicates that procedures in Section 5.2.4.2 will be followed for PIV card (renewals) re-issuance. The procedures in that section are not consistent with paragraphs 2-4 in section 5.2.4.1 and suggest that an expired PIV card and associated certificates will be revoked.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
	Booz Allen Hamilton		G	6.2 pg 53	Need to determine what fits the category of a federal facility and determine applicability Federal "facilities" not owned by the Federal government (i.e., recruiting centers, contractor facilities leased by the Federal Government, etc.)
	Booz Allen Hamilton		G	Table 6-1, p.55-56	Table does not match the text in Sections 6.1.2, 6.1.3, 6.1.4 and 6.1.5
	Booz Allen Hamilton		T	Table 6-1, p.56	Comment in Biometric Authentication row relative to the digital signature on the biometric could be made for all cases where the CHUID is used -- the digital signature on the CHUID could be checked.
	Booz Allen Hamilton		T	Annex A	This section does not include any discussion of validation and certification of biometric capabilities or conformance to biometric standards.
	Booz Allen Hamilton		G	Annex B, Table B-1	In PACS Medium row, PIV Support column, "Digitally Signed Unique Card Identifier" should be "Digitally Signed Unique Cardholder Identifier"
	Booz Allen Hamilton		E	Annex B.2	typo
	Booz Allen Hamilton		T	Annex C	Needs a description of why type-14 logical records are important.
	Booz Allen Hamilton		E	Annex E.2	Add CBEFF

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

Submitted by: _____

Date: _____

Proposed change
* replace all occurrences (throughout the document) of "Position Sensitivity Level" with "Registration Assurance Level". * add the definitions of Registration Assurance Level with levels from OMB 04-04: • Level 1: Little or no confidence in the asserted identity's validity. • Level 2: Some confidence in the asserted identity's validity. • Level 3: High confidence in the asserted identity's validity. • Level 4: Very high confidence in the asserted identity's validity.
Delete first and last bullet
Provide Clarification

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

Submitted by: _____

Date: _____

Proposed change
More detailed explanation of accepted key delivery methods, or a statement indicating that for keys not generated on the PIV card, key delivery is performed via an agency approved out of band method.
Replace last two bullets with: * two fingerprint images; and * one facial image.
Provide Clarification
Card management keys shall meet the minimum algorithm and key size requirements stated in Table 4.1.
Add the reference for [CMS] to Annex F
Either reword statement or add key pair generation and trust anchor storage to the bulleted list above under "Importation and storage of X.509 certificates".
Add a sentence stating that the exportation of X.509 certificates will not be a capability.
Add reference for "Activation by Card Management System" section

Submitted by: _____

Date: _____

Proposed change
Add a section after Section 4.4.5 that indicates that additional CBEFF formatted biometric data may also be stored in the Master File.
Provide Clarification
Add the reference for [RFC 3852] to Annex F
choose and clarify
describe how an application can determine which CBEFF Patron Format is stored on the card

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

Submitted by: _____

Date: _____

Proposed change
Replace the term "authenticated attributes" with "signed attributes".
Add a bullet that says: Specify the Digest Algorithm;
Choose one.
Add a bullet to SignerInfo in both sections that says: Specify the Signature Algorithm;
make consistent.
Provide Clarification
Suggest modifying last sentence in paragraph 1 to read, "In the event of … re-issuance procedures in Section 5.2.4.2 shall be followed to revoke current PIV card and associated certificates." and change 1st sentence in paragragh 2 to "To issue a new PIV card, a new ..."

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

Submitted by: _____

Date: _____

Proposed change
Provide clarification
make consistent.
Add a comment to appropriate rows: Digital signature on CHUID may be checked for higher assurance if..."
Add biometric testing.
Replace Card with Cardholder
delete: [NIST800-3]
Add a paragraph that says that this appendix further defines the fingerprint requirements for biometric enrollment described in Section 4.4.3.
Add: CBEFF Common Biometric Exchange Formats Framework

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