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	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**		Throughout PART 1 it is stated that copies will be maintained by several different entities during the vetting process. This violates the paper reduction act. Also, how long do records have to be maintained? What is the proper method of destruction for these documents? Doesn't multiple copies in multiple offices put the applicant at a higher risk for identity theft? Is it legal to make copies of all forms of identification, believe that there are restrictions within certain states (i.e. driver's licenses, birth certificates), as well as with the social security administration.	Revised to read: "All agencies scan all require documents to include photocopies of two types of identification and fingerprints. Mandate records are scanned on stored on proper diskettes and secure for 3-4 years. After such time, entire records are destroy".
2	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	Introduction, Section 1.3 (Document Organization), pg 2 - 2 para	…..This Standard does not restrict the agenices from adopting additional alternatives. ….are normatie and contain language that is to be followed literally and explicitly in order for agiven implmentation to be deemed compliant with the second part (PIV-II).....	Claification is needed:.. Either all agencies are given limitation to adopt new standards or restriction is set.
12	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE and Carolyn Jackson DS/DFP/DSIS	**T**	FIPS201, PART I, Section 2.1 Page 4	This common PIV card supports the control objectives listed above, and with the Government-side credential issuance process and issuer Certification and Accreditation already established in PIV-I, allows agencies to both trust and use the PIV credentials of other agencies, for physical and logical access control.	Disagree, the PIV card is identity assurance and that is it, it should not be expected that simply having the card entitles any employee physical or logical access to a facility or system.
13	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2 Page 4	For compliance to the PIV-I control objective 1, at a minimum, agencies shall follow the identify proofing resigtration process defined in Sections 2.2.1 - 2.2.4 when issuing identify credentials.	Control Objectives should be number in section 2.1 and outline in this sentence 2.2.1; 2.2.2; 2.2.3; 2.2.4
14	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2 Page 4	It should be noted that one individual shall not assume more than one role in this process	This may work fine with Domestic facilities; but not with overseas. There are domestic and overseas offices that will have an employee performing some or all function.

17	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2 Page 5	PIV Requesting Official - The individual who initiates a request for an identity credential on behalf of the an Applicant;	Revised to read: "**An authorized government** individual who initiates a request for an identity credential on behalf of the an applicant
18	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2 Page 5	PIV Authorizing Offical - The individual who approves the request for an identiy credential;	Revised to read: "**An authorized** government individual who approves the request **from an authorized** PIV Requesting Official for an identity credential on behalf of an applicant"
19	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2 Page 5	PIV Registration Authority - The entity that perform the identity proofing and background checks;	changed named to read: PIV Adjudication Authority.
20	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2 Page 5	PIV Issuing Authority - The entity that issues the identify credential to the Applicant after all identity proofing, background checks, and related approvals have been completed.	Add the word: **authorized** before the word entity. Change name to read: **PIV Credential Authority**
25	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS		FIPS201, PART I, Section 2.2.1 Page 5	At least one of the documents shall be a valid State or Federal Government-issued picture ID.	Unless agencies has a vetting devices/systems to show proof that the ID are valid. Especially for Federal government Ids
26	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2.1 Page 5	The PIV Requesting Official shall submit the PIV request and photocopies of identity source documents for the Applicant to the PIV Authorizing Official.	Revised to read: The PIV Requesting Official shall submit request either electronically (digital Ids or certifcates which allow the requesting official to prove his/her authorized identitiy in electronic transactions) and/or scan document on diskett and foward to the PIV Authorizing Official for approval. Show proof of identity to PIV Requesting Official.
27	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2.1 Page 5	The PIV Authorizing Official shall approve the request and forward it together with photocopies of the identiy source documents to the Registration Authority and the PIV Issuing Authority.	Same issue as above, too many copies of same information, electronic storage of (1) copy. (for those agencies without that capability then they can use the hard copies.
28	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2.1 Page 5	The PIV request shall include: Name, Organization, and contact information of the PIV Requesting Official;	Revised to read: The PIV Request shall include: Name, Position Title, Agency Organization Code, contract number, and agency badge number…….

29	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 5	Name, date of birth, position including the position sensitivity level, and contact information of the Applicant including address of Applicant's parent organization;	Add social security number, contract number,
30	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2.1 Page 5	Name, organization, and contact information of the PIV Authorizing Official;	Revised to read: Name, organization, and contact information of the **government authorized** PIV Authorizing Official
31	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS		FIPS201, PART I, Section 2.2.1 Page 5	Name and contact information of the Registration Authority;	Delete -- To protect the individual conducting the background should not be reveal.
32	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS		FIPS201, PART I, Section 2.2.1 Page 5	Name and contact information of the Issusing Authority, and	Delete - same as above. Protecting the identity of the issuing authority (rename to read Credential Authority)
33	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2.1 Page 5	Signatures of the Requesting and the Authorizing Officials.	Submit through the Digital Ids system -- it is legally approve that the signature is authorized.
34	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 5	Based on the required position sensitivity level, the Applicant shall complete the appropriate background information from listed Table 2-1.	
35	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 6	The Applicant shall provide the completed background information form to the Registration Authority.	
36	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 6	In addition, the Applicant shall appear in person and provide two forms of identity source documents provided earlier to the PIV Requesting Official.	
37	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2.1 Page 6	The Registration Authority shall visually inspect the identification documents and authenticate them as being acceptable.	Once again, strongly urge the use of the term "Adjudication Authority" vs Registration Authority. This person will authenticate the documents based on a visual inspection of the document. Using other authenticate device or system to assist the Adjuicating Official on the true identitiy and validate the documents submitted as proof of identity.

38	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS		FIPS201, PART I, Section 2.2.1 Page 6	The Registration Authority shall subsequently compare the picture on the source document to the Applicant to confirm the Appliant is the holder of the identity source document.	Using other authenticate device or system (such as Identicheck ID device which authenticate ID cards).
39	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 6	Additionally, the Registration Authority shall compare the Applicant information contained in the PIV request (such as full name, date of birth, and contact information) with the corresponding information provided by the Applicant.	
40	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS		FIPS201, PART I, Section 2.2.1 Page 6	At this time, the Registration Authority shall fingerprint the Applicant by collecting all of the Applicant's fingerprints as defined in Section 4.4.3.	This should be conducted by the Adjudication Official only.
41	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE and Carolyn Jackson DS/DFP/DSIS	**G**	FIPS201, PART I, Section 2.2.1 Page 6	The Registration Authority shall conduct the appropriate background check as defined in Table 2-2 using the position sensitivity level from the PIV Request for the Applicant.	Because there may be several offices within an agency that perform the various checks, suggest that instead of saying Registration Authority shall conduct, that you replace with Registration Authority shall ensure that the appropriate background checks are performed as defined..... FYI: The language use for position sensitivity level outline here should be consistent with language currently used.
42	U.S. DEPARTMENT OF STATE	Car	**G**	FIPS201, PART I, Section 2.2.1 Page 6	After successful completion of the appropriate background check, the Registration Authority shall notify the Issuing Authority that the identity credential can be issued to the Applicant.	Revised to read: After successful completion of the appropriate background check, the Adjudication Official shall notify the Issuing Authority the status (complete; denied; suspended; clearance level granted; etc.) Add: Issuing Authority then notify the Requesting/Authorizing Official that the applicant's card is ready for issuance.
43	U.S. DEPARTMENT OF STATE	Gary Schenk GLID Program Manager		FIPS201, PART I, Section 2.2.1 Page 6	Position Sensitivity Level: Low - Authentication of Applicant Identity Source Documents conducted by entity responsible for authorizing PIV card issuance (checking and verifying validity with each Document's issuer). Law enforcement check (fingerprint).	This violates 2.2 where Authorizing Official authenticates documents, that the Registration Authority's job. Fingerprints and background checks.
44	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 6	Position Sensitivity Level: Moderate - National Agency Check and Inquiries (NACI). Refer to Annex D for additional details.	

45	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 6	Position Sensitivity Level: High - NACI and Credit Check (NACIC). Refer to Annex D for additional details.	
46	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 6	Position Sensitivity Level: Critical (Vital National assest-Critical Infrastructure) - Limited Background (LBI) or Background Investigation (BI). Refer to Annex D for additional details.	
47	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 7	The Registration Authority shall be responsible to maintain: Completed and signed PIV Request	
48	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 7	Copies of the identity source documents;	
49	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 7	Completed and signed background form received from the Applicant,	
50	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 7	Results of the required background check, and	
51	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.2.1 Page 7	Any other materials used to prove the identity of the Applicant.	

52	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE Gary Schenk GLID Program Manager Carolyn Jackson DS/DFP/DSIS	G	FIPS201, PART I, Section 2.2.2 Page 7	When issuing or re-issuing identity credentials to current employees, the identity proofing (including the application and approval process) described in Section 2.2.1 shall be followed except that background checks are not required if the results of the most recent previous check are on-file and can be referenced in the applicaton process and verified by the Registration Authority.	One issue that is not addressed is the responsibility of the applicant and/or the Requesting Official to return PIV credential to the Issuing Authority upon terminiation, seperation, death. Also, that the when a PIV card expires, the expired card must be returned before a new card can be issued. Does the applicant need to have biometric images and photo taken again? This document seems to request a copy of the documentation for every step of original process, where is the documentation for the re-issuance process. **Add: expiration date shall be 3 years for contractors or 5 years for government employees at which time another photo shall be required. All other, unless physical change has been made when an applicant shall have a new photo taken.**
53	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE Gary Schenk GLID Program Manager Carolyn Jackson	G	FIPS201, PART I, Section 2.2.3 Page 7	Until the required credential verfication or background investigation is complete, employees and contractors shall not be issued long-term identity credentials but shall be treated according to visitor procedures.	The visitor procedures are not defined in this documentation, and since visitor procedure vary from agency to agency and even facility to facility - suggest that you change verbiage to " shall be treated according to each facility's established visitor procedures." Need to clearly define the term "long-term", suggest not more than 5 years.
54	U.S. DEPARTMENT OF STATE		T*	FIPS201, PART I, Section 2.2.4 Page 7	For citizens of foreign countries who are working for the U.S. Federal Government overseas, a similar process (See Section 2.2.1) for regisration and approval shall be established using a method approved by the U.S. Department of State, Bureau of Diplomatic Security.	
55	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS		FIPS201, PART I, Section 2.3 Page 7	The Issuing Authority shall confirm the validity of the PIV request received from the PIV Authorizing Official and the notification recevied from the Registration Authority.	Submit through the Digital Ids system -- this will confirm the validity of the request from an authorizied government PIV Requesting Authority.

56	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.3 Page 7	The Applicant shall appear in person to the Issuing Authority and present the orginal identity source documents.	
57	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.3 Page 7	Before issuing the identity credential, the Issuing Authority shall verify that the individual who collects the identity credential is indeed the Applicant. (I.e., the Issuing Authority shall compare the Applicant to the original identiy source documents and ensure that the photocopies received from the Authorizing Offical match.)	
58	U.S. DEPARTMENT OF STATE		**G**	FIPS201, PART I, Section 2.3 Page 7	The Issuing Authority shall photograph the Applicant at the time of issuance and retain a file copy of the image.	
59	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.3 Page 7	The identity credential shall then be personalized for the Applicant.	
60	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.3 Page 7	The Issuing Authority shall be responsible to maintain: Completed an formally authorized PIV Request.	
61	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section Section 2.3 Page 7	The name of the PIV identity credential holder (Applicant).	
62	U.S. DEPARTMENT OF STATE			FIPS201, PART I, Section 2.3 Page 8	The credential identifies such as an identity credential serial number.	
63	U.S. DEPARTMENT OF STATE	Carolyn Jackson DS/DFP/DSIS		FIPS201, PART I, Section 2.3 Page 8	The expiration date of the identity credential.	Do you really need an expiration date visually on the card, when it is stored electronically within the system. This will reduce the request of having the card reprinted just to extend to expiration 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)	Proposed change
1	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G		General Comment	HSPD-12 focuses our efforts on protecting "secure Federal and other facilities", this Standard does not require electronic cardholder authentication as required by HSPD-12. Also, nothing less than the High Assurance Profile techniques protect the PIV card from counterfeiting as mandated by directive. The graduated criteria required in the directive must provide PIV authentications within the high assurance profile.
2	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 3 Page 10	The component specifications contained in this standard promote uniformity and interoperability amongst the various PIV systems components, and across agencies and installations.	PIV Part I 2 'Common Identification and Security Requirements' page 4 clearly states "…does not address interoperability of PIV cards and systems among agencies.." If you are going to require interoperability need to remove the sentence in Part I.
3	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3 Page 10	The process specifications contained in this standard serve as a set of minimum requirements for the various activities that need to be performed within an operational PIV system.	
4	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3 Page 10	When implemented in accordance with this standard, the PIV card supports a set of position sensitivity levels and a suite of identity authentication mechanisms that can be used across agencies in a consistent manner.	
5	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3 Page 10	The authenticated identity information can then be used as a basis for access control in a varity of Federal physical and logical access environments.	
6	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3 Page 10	The following sections briefly discuss PIV systems objectives, roles and responsibilities components and their usage, and lifecycle activates of the PIV card.	

7	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	The goal of the PIV system is to provide for a secure and reliable form of Federal employee and contractor identification.	
8	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	This will address the disparities in the quality and security of forms of identification currently used to gain access to Federal facilities.	
9	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	Some of the threats to the current system include the following: Improper issuance of a valid card	
10	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	Use of a stolen or borrowed card to gain access	
11	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	Production of counterfeit cards.	
12	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	Use of a lower sensitivity cards to gain access to more sensitive and critical assets.	
13	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	The following objectives are used to mitigate these threats and guide the development of this standard.	
14	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	Collect and evaluate information sufficient to assure that the legal identity claimed by a PIV Applicant is accurate;	
15	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 3.1 Page 10	Provide a PIV card that may subsequently be used to verify the cardholder (an Applicant who is issued a PIV card) identity rapidly and securely;	Directive is specific with "3(c) can be rapidly authenticated electronically" Suggest you use this verbiage v. rapidly and securely;
16	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 10	Protect the privacy of the cardholder,	
17	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 11	Specify interfaces necessary to read the PIV card efficiently wherever offered by the cardholder when requesting access;	
18	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 11	Provide appropriate security to the entire identity proofing and authentication process;	
19	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 11	Provide protection against use of cloned or counterfeited PIV cards;	

20	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 11	Provide adequate security technology, management procedures, and services to protect the PIV system from being circumvented; and	
21	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.1 Page 11	Support interoperability so that PIV cardholders may be authenticated by any Government facility or information system, regardless of the cardholder's parent organization.	
22	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2 Page 11	Since the PIV system is composed of components and processes across Federal departments and agencies, all entity's involved in identify management play a critical role.	
23	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2 Page 11	This section defines some high-level roles in the system and assigns responsibility to each of them.	
24	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.1 Page 11	Federal departments and agencies that issue and use identity credentials will be responsible for: Establishing position sensitivity levels for Applicants	
25	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.1 Page 11	Authenticating and vetting Applicants for PIV cards;	
26	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.1 Page 11	Authorizing PIV cardholders access to physical facilties and information systems;	
27	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.1 Page 11	Maintaining records of registration and PIV card status information;	
28	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.1 Page 11	Operating and maintaining their portion of the PIV system to assure the objective of this standard; and	
29	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 3.2.1 Page 11	Cooperating with other agencies using the PIV system to control and grant access to all people authorized at the level required by the facility or information system.	This statement implies that having the card inherently grants access to personnel. The card must have the **capability** to be rapidly authenticated electronically, however, local access control grants to either physical or logical systems will be handled by each agency.
30	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.2 Page 11	Applicants are responsible for: Providing authentic identity source documents when requested.	

31	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.2 Page 12	Completing accurately all position and PIV application forms, and	
32	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.2 Page 12	Cooperating in the PIV applicant vetting process and providing biometrics as needed.	
33	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.3 Page 12	Certain agencies have specific responsibilities for implementing this standard:	
34	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.3 Page 12	NIST is responsible for establishing standards, recommendations, guidelines, and conformance tests for components of the PIV system	
35	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 3.2.3 Page 12	OMB is responsible for reviewing and approving PIV system budgets and operational procedures.	Implementation must occur on or before Oct 05, however all agencies have already submitted their FY06 budget requests, so will OMB not fund this project until FY07 or will they be doing passbacks because we weren't able to budget for this new requirement.
36	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.3 Page 12	GSA is responsible for assisting agencies to procure and operate PIV sub-systems.	
37	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.2.3 Page 12	OPM is responsible for assisting agencies to authenticate and verify applicants in accordance with relevant laws and executive orders.	
38	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3 Page 12	An operational PIV system can be logically divided into the following two major subsystems:	
39	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3 Page 12	***PIV System Front-end Subsystem*** **-** the PIV card, card and biometrics readers, and the PIN Pad device. The PIV cardholder interacts with these components in order to gain physical or logical access to the desired Federal resource.	
40	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3 Page 12	***PIV Card Issuance and Management Subsystem*** - the components responsible for identity proofing and registration, card issuance and key management, as well as the various repositories and services (PKI credentials, certificate status servers etc.) required as part of the verification infrastructure.	

41	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3 Page 12	There is another subsystem that becomes relevant when the PIV card is used to authenticate a cardholder who is seeking access to a physical or logical resource.	
42	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3 Page 12	Although this subsystem does not fall within the scope of the standard, various mechanisms for identification and authentication have been discussed within the standard in order to provide consistent and secure means for performing these functions.	
43	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3 Page 12	***Access Control Subsystem*** - the physical and logical access control systems, the protected resources, and the authorization data.	
44	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3 Page 12	The Figure 3-1 illustrates the functional model for the operational PIV system, identifying the various system components and the direction of data flow between these components.	
45	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	The PIV card issued to the Applicant upon completion of all registration processes.	
46				FIPS201, PART 2, Section 3.3.1 Page 14	This PIV card has a "credit card" sized form factor, with one or more embedded integrated circuit chips (ICC) that provide memory capacity as well as computational capability.	
47	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	This PIV card is the primary component of the PIV system and is used by its holder for authentication to various physical and logical resources.	
48	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	Card readers are located at the access points for controlled resources where a cardholder may wish to gain access (both physical and logical_ by using the PIV card.	
49	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	The reader communicates with the PIV card to retrieve the appropriate information, located on the memory of the card, in order to pass it into the access control systems for granting or denying access.	
50	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	Card writers are very similar to the card readers and are used for personalization and initialization of the information that needs to be stored on the PIV cards.	

51	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	The data to be stored on PIV cards include personal information, certificates, the Personal Identification Number (PIN), biometric data and is discussed in further detail in later sections.	
52	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	Similar to the card reader, the biometric reader may be located at secure locations where a cardholder may wish to gain access by using the PIV card.	
53	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	Biometric readers depend upon the used of stored biometric data of the cardholder stored in the memory of the card and it's comparison of a real-time biometric sample.	
54	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	The use of biometrics provides an additional factor of authentication (Something you are), in addition to providing the card (something you have)	
55	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	As with a biometric reader, a PIN pad device can also be used along with the card readers at secure locations where a higher level of authentication assurance of the cardholder is required.	
56	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	The cardholder presenting the PIV card must type in their PIN into the PIN pad.	
57	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.1 Page 14	The Pin pad therefore also supports the use of an additional factor of authentication (something you know), in addition to providing the card (something you have) to provide a higher level of authentication assurance.	
58	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 14	The Identity Proofing and Registration component in Figure 3-1 refers to process of collection, storage, and maintenance of all information and documentation that that is required to authenticate and assure the identity of the applicant.	
59	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 14	Information such as the full name, address, date of birth, marital status, Federal designation, sponsor identify, and biometric information, are examples of information collected from the Applicant at the time of registration.	

60	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 14	All of the Applicant registration data collected at the onset of the registration process including the biometric data, as well any updates to this information during the usage of this card, is stored in the Registration Repository.	
61	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 14	The security mechanisms available on a PIV card may be used in a challenge response protocol to verify the authenticity of the card an the cardholder.	
62	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 14 & 15	The generation of the key pairs, distribution of digital certificates containing the public key of the cardholder, management of the certificates so that application can be prohibited from using certificates which are no longer valid, are all part of the Key Management component.	
63	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 15	This Key Management component are used throughout the lifecycle of the PIV cards from issuance of Public Keys Infrastructure (PKI) credentials, to usage of PKI credentials for secure operations, to eventual re-issuance or termination of the card.	
64	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 15	Key Management is also responsible for the provisioning of publicly accessible repositories and services (such as the PKI repository) that inform the requesting application on the status of these PKI credentials.	
65	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 15	The Card Issuance component primarily deals with the personalization of the physical (visual surface) and logical (connect of ICC) aspects of the card.	
66	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 15	This includes printing of photographs, name and other information on a the card as well as loading the relevant card applications, biometric and other data.	
67	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.2 Page 15	The PIN to unlock the card may also be collected from the Applicant or generated at the time of issuance, and embedded within the PIV card.	
68	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.3 Page 15	Physical and logical resources are the end targets of the entire PIV system.	

69	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.3 Page 15	A physical resource is the secured facility (building entrances, rooms, turnstiles, parking gates, etc) that the cardholder desires to access.	
70	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.3 Page 15	The logical resource is typically a location n the network (e.g., computer workstations, folders, files, database records, or software programs) to which the cardholder desires to gain access.	
71	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.3 Page 15	The authorization data component for both the physical and logical resource is populated with relevant cardholder access information. An example of this can be a simple Access Control List (ACL).	
72	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.3 Page 15	The physical and logical access control systems grants or denies access to a particular resource and includes and Identification and Authentication (I&A) component as well as a authorization component.	
73	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.3 Page 15	The I&A component interacts with the PIV card and uses mechanisms discussed in the Section 6 to identify an authenticate cardholders.	
74	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.3.3 Page 15	Once authenticated, the authorization information to component interacts with the authorization data component to match the cardholder provided with the card reader, and the authorization data, PIN pad device, certificate status services, and optionally with the biometric reader.	
75	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 15	The PIV card lifecycle primarily consists of seven activities. These activities that take place during fabrication and pre-personalization of the card at remanufactures are not considered a part of this lifecycle model.	
76	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 15	Figure 3-2 presents these PIV activities and shows the PIV card request as the initial activity and PIV card termination as the end of the life.	

77	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 16	***PIV card request*** - This activity deals with the initiation of a request for the issuance of a PIV card to an applicant by the PIV Requesting Official as well as the validation of this request by the PIV Authorizing Official.	
78	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 16	***Identity proofing and registration*** - the goal of this activity is to verify claimed identity of the Applicant and that the entire set of identity source documents presented at the time of registration is valid. On successful validation of these documents the Applicant is enrolled into the agency's PIV Management System.	
79	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 16	***PIV card issuance*** - This activity primarily deals with the personalization (physical and logical) of the card and the issuance of the card to the intended Applicant.	
80	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 16	***PKI credential issuance*** **-** This activity deals with generation of logical credentials and loading them onto the PIV card.	
81	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 16	***PIV card usage*** - the main purpose of issuing a PIV card is so that a cardholder can be authenticated or verified at a later point in time before providing physical or logical access. Access authorization decision s can then be made once the cardholder is successfully authenticated as part of this phase.	
82	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 16	***PIV card maintenance*** - This activity deals with the maintenance or update of the physical card as well as the data such as various card applications, PIN, PKI credentials and biometric stored on it.	
83	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 3.4 Page 16	***PIV card termination*** - The termination process is used to permanently destroy or invalidate the usage of the card including the data on it including the keys such as that it cannot be used again.	
84	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4 Page 17	This section identifies the requirements for the components of the PIV system. The requirements for the PIV card layout, card data object, card reader, and biometrics are provided below.	

85	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1 Page 17	Section 4.1 provides the physical and logical card specifications. The PIV Cardholder Unique Identification (CHUID) object is described in Section 4.2. Cryptographic keys associated with the cardholder are described in Section 4.3. Formats for mandatory biometric information is defined in Section 4.4	With all the requirements contained in this document there will barely be enough room on a 64k card to store the minimum requirements. This will force agencies to go to a higher kilobit smart card causing an undue financial and resource strain on agencies.
86	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1 Page 17	Sections 4.1.1 - 4.1.3 provides a description of applicable standards, tamper proofing requirements, and physical characteristics of the PIV Card. Section 4.1.4 describes the card topography. Section 4.1.5 provides the PIV card data storage requirements. Finally activation of logical credentials on a PIV card is described in Section 4.1.6.	The PIV card specifications described herein exceed the GSC-IS version 2.1. Industry will not be able to supply the product to meet this requirement and distribute to all federal agencies by OCT 05, so agencies are precluded from being able to meet the implementation date. You are asking us to buy a product that does not exist yet.
87	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1 Page 17	The side of the card that contains the contacts if referred to as the front of the card and the other side is referred to as the back of the card. The PIV card shall comply with physical characteristics as delineated in ISO/IEC 7810, ISO/IEC 10373, ISO/IEC 7816 for contact cards, and ISO/IEC 14443 for contactless cards. Any manufacturing process required to meet the requirements in the standard shall met the specified standards and shall result in a flat card.	PACS v2.2 states that, at present, non-prioetary contactless technology does not support symmetrical keys. To be compliant, PACS further states "a High Assurance Profile implementation must use the ISO 7816-4 and 7816-8 APDU commands.." Currently, this mean that only contact cards can implement a conformant High Assurance Profile" Additionally, contactless cards for logical PKI are only available in limited vendor-proprietary implementations. Submit that the use of contactless card technology does not meet HSPD in that only a High Assurance Profile can provide true card authentication. While HSPD may appear ambiguous in this content, the Standard defines Low and Medium Assurance Profiles that violate the precepts of HSPD-12 3(b) and (c).
88	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.1a Page 17	The printing shall not rub off during the life of the PIV card nor deposit debris on the plastic card printer rollers during printing and laminating.	

89	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.1b Page 17	Printed material shall not interfere with contact and contactless placement or impede action the contents therein.	
90	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.2a Page 17	A tri-modal or bi-modal optical variable device (OVD) or optical variable ink (OVI) shall be embedded in the card material on the front of the card.	
91	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.2a Page 17	The OVD or OVI shall be such that it is transparent when looking at it directly and changes colors as the viewing angle changes.	
92	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.2a Page 17	Incorporation of this feature within the card body shall be free of defects, such as fading, discoloration, or continuation as determined by visual inspection.	
93	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.2b Page 17	Additional tamper resistance and anti--counterfeiting methods may be incorporated at an agency's discretion. Federal agencies are strongly encouraged to review the viability, effectiveness, and currency of these tamper resistance and anti-counterfeiting methods.	
94	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.3a Page 17	The PIV card shall contain a contact and contactless ICC interface.	Contactless card technologies do not meet HSPD-12 objectives, why would you require it on the card when it would be an unused resource that would just increase the cost of card. For those agencies who use contactless technologies for uses other than physical or logical access they should be allowed to maintain it on the card, however, it should not be mandated.
95	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3b Page 18	The card body shall be a polyvinyl chloride (PVC) PVC core with polyethylene terephthalate (PET) layers or a similar card material type satisfying the durability requirements specified in (ANSI322) and ISO/IEC 7810.	
96	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3c Page 18	The card shall be 27 to 33 mil card thickness (prior to lamination) in accordance with ISO/IEC 7810.	

97	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3d Page 18	The cards shall be subjected to (ANSI1322). While the (ANSI1322) test methods do not currently specify compliance requirements, the tests shall be used to compare card durability and performance.	
98	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3d Page 18	The (ANSI1322) tests minimally shall include; card flexure, static stress, plasticizer exposure, impact resistance, card structural integrity, surface abrasion, temperature and humidity induced due migration, ultraviolet light exposure, a laundry test and optional magnetic stripe abrasion.	
99	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3e Page 18	At the agency's discretion, the card may be required to be resistant to chemical effects arising from use in a flight line or equal austere environment.	
100	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3f Page 18	The PIV card shall not be embossed.	
101	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.3g Page 18	The PIV card shall not be punched with holes or physically altered in any similar fashion.	The Department has found that when cards are not punched and placed on a chain employees lose them repeadtly. The type of plastic case required to prevent such loss, should the card not have a hole in would increase the overall cost of the card per PIV cardholder tremendously. Suggest that a standard hole size and location be determined for the card should agencies budgets restrict the use of the additional card holder. ID's are required to be visible while in a Government facility so this is not simply something you can put in and out of your wallet like a credit card.
102	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3h Page 18	Decals shall not be adhered to the card.	
103	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3i Page 18	The cardstock shall withstand the effect of high temperature required by the application of a polyester laminate on one or both side of the card by commercial, off-the-shelf (COTS) equipment.	

104	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3i Page 18	The cardstock shall allow production of a flat card in accordance with (ISO7810) after lamination of one of both sides of the card.	
105	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3j Page 18	Cards shall not malfunction or delaminate after hand cleaning with a mild soap ad water. The reagents called out in Section 5.4.1.1 of (ISO10373) shall be modified to include a 2% soap solution. The card shall be deemed acceptable if it meets these cleaning requirements.	
106	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3k Page 18	The card shall be subjected to actual, concentrative or artificial sunlight to appropriately reflect 2000 hours of Southwestern United States sunlight exposure in accordance with Section 5.12 of (ISO10371). Concentrated sunlight exposure shall be performed in accordance with (G90-98), and accelerated exposure in accordance with (G155-00). After exposure, the card shall be subjected to the (ISO10373) dynamic bending test and shall have no visible cracks or failures. Alternatively, the card may be subjected to the (ANSI1322) tests for ultraviolet and daylight fading resistance and subject to the same (ISO10373) dynamic bending tests.	
107	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.3l Page 18	In the case that OVDs are used as a tamper resistant feature, the minimum peel strength requirement in (ISO7810) may not met for the OVD patch in the layer of the cardstock that contains it and as such the minimum peel strength requirement shall be addressed on a case-by-case basis. However, the remainder of the cardstock layer with the OVD and the remainder of the card body shall meet all requirements of (ISO7810).	
108	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.4 Page 19	The information on a PIV card shall be in both visual and electronic form. This section does not cover information stored in the ICCs. This standard does not specify whether a single chip or multiple chips are used to support the mandated contact and contactless interfaces.	Suggest you change to say - the PIV cardholder information shall be in both visual and electronic form, you have many things on the electronic side that would be impossible to provide a visual display of - such as the fingerprints, pki certificates etc.

109	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.1 Page 19	A pictorial representation of the mandatory and optional visual information on the front of the card is provided in figure 4-1. The placement of Zones shall be printer on the card as designated.	
110	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.4.1 Figure 4-1 Page 19	Zone 1 - Photo. Minimum 1.08" x 1.45" 1 full face frontal pose from top of head to shoulder. Uniform light blue background. Border frame (optional). Minimum 300 dpi.	Disagree strongly with the requirement of a light blue background, should be optional not mandatory.
111	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.1a Page 19	Zone 1 - Photograph. The photograph shall be placed in the upper left corner. The photo will be placed such that it does not conflict with contact or contactless chip placement. The photograph shall be a full frontal pose from top of head to shoulder. The minimum size shall be 1.08 inch wide and 1.45 in length although larger photos will better facilitate visual verification. A minimum of 300 dpi resolution shall be required. A photo border frame is optional.	
112	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.4.1b Page 19	Zone 2 - Name. The surname and first names shall be printed under the photograph in capital letter in the order depicted. The font shall be Arial Bold of minimum 10pt size.	The issue of middle initials are not addressed, there are several John Smith's within our agency as we are sure you have employees with same name as well, suggest that middle initial be printed on card if PIV individual has one to further provide visual clarification of ownership.
113	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.1c Page 19	Some 8 - Employee Affiliation Employment Identifier. The employee affiliation, such as "CONTRACTOR", "ACTIVE DUTY", "CIVILIAN" or an Agency-specific employee identified or nomenclature, shall be printed in the Arial Bold Black font of minimum 7 pt size.	
114	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.4.1d Page 20	Zone 9 - Text "United States Government". The "UNITED STATES GOVERNMENT" text shall be printed on the top from portion of the card and shall be capitalized in the Arial Bold Black font of minimum 7pt size.	The text UNITED STATES GOVERNMENT is mandatory, yet the agency name is optional, the agency name should be mandatory and the text UNITED STATES GOVERNMENT should be optional.

115	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.4.1e Page 20	Zone 14 - Expiration Date. The card expiration date shall be printed in the lower right hand corner of the card in the ISO/IEC 8601 format YYYY/MM. The font for the text "Expires" shall be Arial Black of minimum 6pt size. The font for the date shall be Arial Black of minimum 10pt size.	When you just put in the year and month this confuses employees, does my badge expire on the first or last day of the month displayed? Suggest the format of MM/DD/YY be used for full clarification of expiration. Also, contractors may have contractors that end in the middle of the month so the actual day of expiration is critical to maintain assurance that only those PIV cardholders with 'active' cards are permitted into facilities or systems.
116	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.2 Page 20	Back of the Card (Mandatory) - the pictorial representation of the mandatory visual information on the back of the card is provided in Figure 4-2. The standard specifies a different format for the back of PIV card issued to the military, in accordance with the Geneva Convention format as depicted in Figure 4-2. the description of all visual information items follows. Please not that he diagrams below are not to scale.	
117	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.2a Page 21	Zone 1 - Agency Card Serial Number. The first line in Figure 4-2 shall print the issuing Agency's cards unique serial number. The format for this serial number shall be at discretion of the issuing Agency.	
118	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.2b Page 21	Zone 2 - Issuer Identification. The second line in Figure 4-2 shall print the issuer identifier, consisting of six characters for the Department Code, four characters for the Agency Code and a five-digit number that uniquely identifies the issuing facility within the agency.	
119	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3 Page 21	Front of the Card (Optional) The description of optional information in Figure 4-1 follows.	
120	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3a Page 21	Zone 3 - Signature. The agency may print the cardholder signature below the photograph and cardholder name. The space for the signature shall not interfere with the contact and contactless placement requirements.	

121	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3b Page 21	Zone 4 - Pay grade. The pay grade for the cardholder may be printed in this area in a format determined by the issuing Agency.	
122	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3c Page 21	Zone 5 - Rank. The rank of the cardholder may be printed here in a format determined by the issuing agency.	
123	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3d Page 22	Zone 6 - bar code. A bar code may be placed left side of the card surface if applicable to the issuing agency. The agency using (PDF417) bar code shall use this location. This placement shall be as depicted in the diagram (I.e. left side of the card).	
124	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3e Page 22	Zone 10 - Agency Name and/or Department. The name of the Agency and/or the cardholder's department may be printed here. The font shall be Arial black of minimum 7pt size.	
125	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3f Page 22	Zone 11 - Agency Seal. The seal for the issuing Agency may be printer on the upper right side of the card. The font shall be Arial Black minimum 7pt size.	
126	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3g Page 22	Zone 12 - Emergency Response Official Identification. The agency may print "Federal Emergency Response Official" above the chip but not in conflict with the contactless placement requirements.	
127	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.3h Page 22	Zone 13 - Issue Date - The date of card issuance may be printed above the expiration date in the ISO/IEC 8601 format YYYY/MM. The font for the text "Issued" shall be Arial Black of minimum 6pt size. The font for date shall be Arial Black of minimum 10pt size.	
128	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.4 Page 22	Back of the Card (optional) - the description of optional information in Figure 4-2 follows.	
129	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.4 a Page 22	Zone 3- Magnetic Stripe. The card may contain a magnetic stripe. The magnetic stripe shall be high coercivity and placement will be in accordance with ISO/IEC 7811.	

130	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.4 b Page 22	Zone 4 - Return to. The card may contain a language indicating where the card should be returned if found.	
131	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.4 c Page 22	Zone 5 - Physical Characteristics. The cardholder's physical characteristics such as height, eye color, and hair color may be printed on the back of the card in Aril Black font of minimum 7 pt size.	
132	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.4 d Page 22	Zone 6 - Standard Language for Emergency Responder. The standard language for emergency responder may be printed on the back of the card in Arial Regular font of minimum 5pt size. The printed statement shall read "The bearer of this card is a designated Emergency Responder. After credential verification, bearer should be given access to controlled areas."	
133	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.4 e Page 22	Zone 7 - Standard Section 499, Title 18 language. The standard section 499, Title 18 language warning against counterfeiting, altering, or misusing the card may be printed below the issuer identification in Arial Regular font of minimum 6pt size.	
134	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.4.4 f Page 22	Zone 8 - Instructions for Return of Lost Card. Instructions for returning lost cards may be printed on bottom back of the card. The font used for instruction information shall be Arial regular font of minimum 6pt size. The font used for return address information shall be Arial Regular of minimum 5pt size.	The word "font" is misspelled as "front" change to font.
135	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.4.4 g Page 22	Zone 9 - Linear 3 of 9 Bar Code. The left corner (from top to bottom) may be used to print bar code. The bar code type shall be of a 3 of 9 barcode in accordance with Association for Automatic Identification and Mobility (AIM) standards.	

136	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	Logical Credential Data Model. In order to support a variety of authentication mechanisms, the PIV Logical Credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity via the authentication mechanisms specified at each assurance level.	
137	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	These mandatory data elements collectively comprise the data model for PIV Logical Credentials, and include the following.	
138	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.5.1 Page 23	A Personal Identification number (PIN)	We are talking logical here, yet the word PIN is described a physical number used to gain access to a physical access control system, to use the term for both physical and logical there needs to be some distinction between the use of the word or use a different word for each.
139	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	A Cardholder Unique Identification object (CHUID)	
140	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	One asymmetric key pair and corresponding certificate associated with the cardholder,	
141	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	Two biometric fingerprints; and	
142	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.5.1 Page 23	Biometric facial image.	This may cause an issue with Foreign Nationals and violate current Foreign Policy's and agreements with other countries. With over 250 facilities overseas this could be a huge issue for State Department.

143	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	PIV logical credentials fall into three categories: credential elements used to prove the identity of the cardholder to the card (CTC authentication), credential elements used to prove the identity of the card management system to the card (CMTC authentication), and credential elements used by the card to provide the identity of the cardholder to an external entity (CTE authentication) such as a host computer system.	
144	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	PINs fall into the first category, card management keys in the second category, and the CHUID, biometric information, symmetric keys, and asymmetric keys fall into the third. Biometric information may optionally be used in CTC authentication if the PIV card implements on-card matching of biometric information.	
145	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	The PIV data model may be extended to meet agency-specific requirements. This specification establishes requirements for 4 classes of optional logical credentials.	
146	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	An asymmetric key pair and corresponding certificate for digital signature;	
147	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	An asymmetric key pair and corresponding certificate for key management;	
148	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	Asymmetric or symmetric keys for supporting additional physical access applications; and	
149	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.1 Page 23	Symmetric key(s) associated with the card management system.	

150	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.2 Page 23	File Structure. The PIV card architecture described in (SP800-73) defines a Cryptographic Information application (CIA) in Section 7.1 that contains information about cryptographic keys and other authentication objects that comprise the PIV cardholder's Logical Credentials.	
151	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.2 Page 23	A host system can obtain all the information it needs to locate and retrieve biometric information from the card, or to select specific cryptographic keys stored on the card for subsequent cryptographic computations used in challenge-response operations.	
152	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.2 Page 23	The host system can therefore dynamically discover the location and file identifiers associated with the Logical Credentials data elements, without the need for a prior knowledge of these.	
153	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.2 Page 23 & 24	However, the CHUID and biometric information shall be stored as transparent files in the root file system of the Card Manager (the Master file) to facilitate rapid retrieval for physical access control applications.	
154	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.2 Page 24	It is important to note that the CIA may contain information about other authentication objects associated with applications on the PIV card that are not specified in this standard	
155	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.5.2 Page 24	This standard only addresses authentication objects that are part of the PIV Logical Credentials.	
156	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6 Page 24	PIV Card Activation. The PIV card muse be activated to perform privileged operations.	
157	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6 Page 24	The PIV card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system.	

158	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6 Page 24	Cardholder authentication is described in Section 4.1.6.1 and Card Management system authentication is described in Section 4.1.6.2.	
159	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.1.6.1 Page 24	Activation by Cardholder. Every PIV card shall implement PIN-based cardholder activation	What are the requirements for the PIN, are we to use FIPS PUB 140-2 or FIPS-112 or some other standard. Need to clarify the requirement for the PIN, such a length, upper/lower case etc.
160	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	PIV cards may optionally implement activation using biometric information stored on the card.	
161	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	For PIN-based cardholder activation, the cardholder shall supply a numeric PIN. The PIN shall be transmitted to the PIV card and checked by the card.	
162	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	If the presented PIN is correct, the PIV card is activated. The PIV card shall include mechanisms to limit the number of guesses an adversary can attempt if a card is lost or stolen.	
163	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	The Pin authentication used by cardholders to activate the PIV card shall meet the identity-based authentication requirements of FIPS PUB 140-2 (I.e. Level 3 Operation Authentication).	
164	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	For biometric-based cardholder activation, the cardholder shall present biometric information (e.g. a fingerprint) to a reader.	
165	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	The biometric information shall be transmitted to the PIV card, and using biometric match-on-card, compared with the stored biometric information (e.g. image or template).	
166	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	If the presented biometric matches the stored biometric, the PIV card is activated.	
167	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	This specification does not prescribe the type of biometrics used for card activation, nor the algorithms or techniques for performing the biometric comparison.	

168	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	The biometric data used for card activation is a local decision within each department or agency.	
169	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.1 Page 24	Where inter-agency interoperability is a concern, agencies that use biometric-based cardholder activation in house should also provide a PIN pad for card activation.	
170	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.2 Page 24	Activation by Card Management System. PIV cards may support card activation by the card management system to support card personalization and post-issuance card update.	
171	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.2 Page 24	To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card as specified in (GP).	
172	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.2 Page 24	When cards are personalized, card management keys shall be sort to be specific to each PIV card. That, is a card issues may not use a single cryptographic key to activate more than one card.	
173	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.1.6.2 Page 24	If supported, card management keys shall meet the algorithm and key size requirements stated in Table 4-1.	
174	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2 Page 25	Cardholder Unique Identifier (CHUID). The PACS implementation Guidance (PACS) defines the Cardholder Unique Identifier (CHUID).	
175	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2 Page 25	The CHUID includes a data element, the Federal Agency Smart Credential Number (FACS-N), which uniquely identifies each card.	
176	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.2 Page 25	The PIV card shall include an elementary file container continuing the CHUID, as defined in (PACS).	Change the word continuing to containing
177	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2 Page 25	The PIV CHUID includes two additional data elements specific to this standard, and is digitally signed by the issuing authority.	

178	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2 Page 25	CHUID data elements specific to this standard are described below in Section 4.2.1. The format of the CHUID signature element is described in Section 4.2.2. Below.	
179	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2 Page 25	The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV card without card activation.	
180	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2 Page 25	The PIV FASC-N may not be modified post-issuance.	
181	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.1 Page 25	PIV CHUID Data Elements. In addition to the mandatory FASC-N that will uniquely identify a PIV card, the CHUID shall include an expiration date and a position sensitivity level.	
182	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.1 Page 25	The expiration date data element will, in machine readable format, specify when the card expires to facilitate status checking and the asymmetric signature field.	
183	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.1 Page 25	The expiration date and position sensitivity level were not included in (PACS); this specification uses tags that were reserved for future use for this data (see Table 4-2) and defines encoding rules for these data elements. (see Table 4-3)	
184	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.2.1 Page 26	In addition, (PACS) does not specify a format for the asymmetric signature field. For PIV cards, the format of the asymmetric signature field is specified in Section 4.2.2.	It has been determined that any level below high assuranace does not comply with HSPD-12, in addition PACS does not specify a format for the asymmetric signature field because it was determined that it use is not acceptable even prior to this Directive. To meet the directive objectives each agency regardless of their facility security level must meet the high assurance profile to be in compliance. Recommend that the use of symmetrical key be mandated with cardholder data input comparison to establish true card authentication for physical access control, which mets the directives objective.

185	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.2.2 Page 26	Asymmetric Signature Field in CHUID. This specification requires inclusion of Asymmetric Signature filed in the CHUID container.	Asymmetric should not be an option in order to met the directive.
186	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.2.2 Page 26	(PACS) specified a tag for the Asymmetric Signature data element, but does not specify the format.	Asymmetric should not be an option in order to met the directive.
187	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.2.2 Page 26	The Asymmetric Signature data element of the PIV CHUID shall be formatted as the Cryptographic Message Syntax (CMS) external digital signature, as defined in (CMS).	Asymmetric should not be an option in order to met the directive.
188	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.2.2 Page 26	The digital signature shall be computed over the entire contents of the CHUID, excluding the Asymmetric Signature Field itself.	Asymmetric should not be an option in order to met the directive.
189	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.2.2 Page 26	The signature shall be generated by the Issuing Authority using the Issuing Authority's PKI private key.	PKI Access Certificate is not an acceptable method for access control due to its response latency, especially for a worldwide agency.
190	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	Algorithm and key size requirements for the asymmetric signature are detailed in Table 4-4.	
191	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	The CMS external digital signature must contain the following elements:	
192	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	Content shall be encoded in *SignedData*;	
193	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	Certificates and Certificate Revocation List (CRLs) shall not be included in the message;	
194	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	*SignerInfos* shall be present and include only a single *SignerInfo*;	
195	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	The *SignerInfo* shall:	

196	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	Use the issuerAndSerialNumber choice for SignerIdentifier.	
197	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	Specify the Digest Algorithm	
198	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	Include the digital signature.	
199	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	The public key required to verify the digital signature shall be available as an X.509 certificate.	
200	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.2.2 Page 26	The certificate shall be a digital signature certificate issued under (COMMON), and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Section 4.3	
201	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	At a minimum, the PIV card must store one asymmetric private key, a corresponding public key certificate, and perform cryptographic operations using the asymmetric private key.	
202	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	Cryptographic operations with this key are only performed through the contact interface.	
203	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	Asymmetric private keys shall be 1024 or 2048-bit RSA keys, or elliptic curve keys f corresponding strength (160 or 224-bit respectively).	
204	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	The PIV card shall implement the following cryptographic operations and support functions:	
205	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	RSA or elliptic curve key pair generation	

206	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	RSA or elliptic curve private key cryptographic operations	
207	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.3 Page 27	Importation and storage of X.509 certificates	Importing and storing the X.509 certificates for use in PKI path validation violates the FBCA Certificate Policy requirement ha the path must be discovered each time before it can be validated.
208	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	The PIV card may include additional asymmetric keys and PKI certificates. This specification defines requirements for digital signature and key management keys.	
209	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	Where digital signature keys are supported, the PIV card is not required to implement a secure hash algorithm (e.g., SHA-1).	
210	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	Message hashing may be performed off-card. As above, useful optional functions include key pair generation and trust anchor storage.	
211	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	No cryptographic operations are mandated for the contactless interface, but agencies may choose to supplement the basic functionality with storage for a local authentication key and support for a corresponding ser of cryptographic operations.	
212	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	That is, if an agency wishes to utilize an AES-based challenge response for physical access, the PIV card must contain storage for the AES key and support AES operations through the contactless interface.	
213	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	If the contactless interface require storage for a corresponding public key certificate.	
214	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	All cryptographic operations using the PIV keys shall be performed on-card; the PIV card need not implement any additional cryptographic functionality (e.g., hashing, signature verification, etc.) on-card.	

215	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	When used to protect access to sensitive data and systems, this functionality may be augmented (e.g., with hash algorithms and signature verification) by a validated software cryptographic module.	
216	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	The PIV card has a single mandatory key and four type of optional keys:	
217	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	The PIV authentication key is a asymmetric private key supporting logical and physical access and is mandatory for each PIV card;	
218	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	The l*ocal authentication* key may be either a symmetric (secret) key or an asymmetric private key for physical access and is optional;	
219	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	The *digital signature* key is an asymmetric private key supporting document signing and is optional;	
220	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 27	The *key management* key is an asymmetric private key supporting key establishment and transport and is optional; and	
221	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28	The *card management* key is a symmetric key used for personalization and post-issuance activities.	
222	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28	All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above.	
223	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28	All PIV cryptographic keys shall be stored within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above.	
224	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28	In addition to an overall validation of Level 2, the PIV card shall provide Level 3 physical security to protect the PIV private keys in storage.	

225	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28	Algorithms and key sizes for each PIV key type are specified in the following table.	
226	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28	Requirements specific to each storage and access of each class of keys are detailed below. Where applicable, key management requirements are also specified.	
227	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28	The PIV Authentication Key - The PIV Authentication key shall be generated on the PIV card.	
228	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28	The PIV card shall not permit exportation of the PIV authentication key.	
229	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 28 & 29	The PIV authentication key must be available only through the contact interface of the PIV card.	
230	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The PIV card key operations may be performed using an activated PIV car without explicit user action (I.e., the PIN need not be supplied for each operation.)	
231	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The PIV shall store a corresponding X.509 certificate to support validation of the public key.	
232	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The X.509 certificate shall include the FAC-N in the subject alternative name extension to support physical access procedures.	
233	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The expiration ate of the certificate must be no later than the expiration date of the PIV card.	
234	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	Section 5.2.3 of this document specifies the certificate format and the key management infrastructure for PIV authentication keys.	

235	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	Local Authentication Key - The PIV card shall not permit exportation of the local authentication key. The local authentication key is used solely for physical access (e.g., to support PACS High Assurance authentication). Private/secret key operations may be performed using this key without explicit user action (i.e., the PIN need not be supplied.)	
236	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	Cross-Agency interoperability is not a goal for the local authentication key. Consequently, this document does not specify key management protocols or infrastructure requirements.	
237	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The Digital Signature Key - The PIV Digital Signature key shall be generated on the PIV Card. The PIV card shall not permit expiration of the digital signature key. If present, the digital signature key must only be accessible using the contact interface of the PIV card. Private key operations may be performed using an activated PIV card with explicit user action (i.e., the PIN must be supplies for each private key operation.)	
238	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The PIV card shall store a corresponding X.509 certificate to support validation of the digital signature key. Section 5.2.3 of this document specifies the certificate format and the key management infrastructure for PIV digital signature keys.	
239	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The Key Management Key - the PIV Key Management key may be generated on the PIV card or imported to the card. If present the key management key must only be accessible using the contact interface of the PIV card. Private key operations may be performed using an activated PIV card without explicit user action (i.e., the PIN need not be supplied for each operation.)	

240	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The PIV card shall import and store a corresponding X.509 certificate to support validation of the key management key. Section 5.2.3 of this document specifies the certificate format and the key management infrastructure for PIV key management keys.	
241	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The Card Management Key - the Card Management key is imported onto the card by the issuer. If present, the card management key must only be accessible using the contact interface of the PIV card. See Section xx ("Activation by Card Management System") for further details.	
242	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.3 Page 29	The PIV card may also import and store X.509 certificates for use in PKI path validation. These trust anchor certificates may be accessed through the contact interface using an activated PIV card without explicit cardholder action. If supported, initialization and update of trust anchor certificates shall require explicit cardholder action, in addition to activation of the card.	
243	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Biometric Specifications. The biometric data shall be collected and used as follows:	
244	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Ten fingerprints to support law enforcement check during application process,	
245	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Two electronic fingerprints to be stored on the card for automated verification process, and	
246	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	An electronic facial image to be stored on the card for alternate identity verification process.	
247	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.4 Page 30	Recognition accuracy rates for fingerprint and facial images have been established by NIST in large-scale trials.	For Logical Access, the biometric requirement should permit use of templates with a minimum accuracy level exceeding a minutiae only template.

248	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Fingerprints shall be primary biometric utilized in the PIV system, as they provide significantly higher accuracy.	
249	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	The recognition rates or facial image is much lower than those of fingerprints images, as it is sensitive to external conditions like illumination and pose.	
250	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Index fingerprints are preferred for verification purposes. In case of difficulty in getting index finer prints, an alternate set of finger-pairs could be used in the following decreasing order of preference:	
251	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Thumb	
252	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Middle Finger	
253	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Ring Finger	
254	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	Little Finger	
255	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	The two fingers should not be from the same hand if practicable.	
256	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	To improve robustness of the fingerprint recognition systems and data interoperability, the format for the storage and exchange of the biometric information captured and used in the PIV system shall conform to established standards.	
257	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	For PIV, one-to-many fingerprint matching shall be performed during the Application process.	

258	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	One-to-one fingerprint matching shall be performed for PIV identity verification.	
259	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4 Page 30	The biometric data on the PIV card may only be read from an activated card through the contact interface.	
260	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.1 Page 30	PIV Registration (Biometric enrollment) and Issuance. For the detection of duplicate credentialing and background screening, the PIV registration (biometric enrollment) process requires a one-to-many *biometric identification* search.	
261	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.1 Page 30	The biometric data supplied for biometric identification search shall consist of a complete set of ten "slap" fingerprints which may alternatively be accompanied by a set of ten rolled fingerprint images.	
262	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.1 Page 30	Although the specific tasks involved in identity-proofing are incremental with respect to the sensitivity-level of the employee or contractor position, law enforcement checks supported by biometric identification are common to all sensitivity levels.	
263	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.1 Page 31	During card personalization, the biometric data from two fingers and a facial image shall be embedded in the PIV card for comparison purposes in subsequent authentication/verification attempts.	
264	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.1 Page 31	All biometric data shall be digital signed by the Issuing Authority. Fingerprint quality and format shall be as described in Section 4.4.2.	
265	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.1 Page 31	Facial image quality and format shall be as described in Section 4.4.5 It is also recommended that biometric verification (one-to-one matching) be performed between the enrolled image and a live sample prior to issuance of the card. This improves the confidence in the integrity of authentication during actual card usage.	

266	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	Fingerprint Representation. Currently. The only representations of fingerprint data that has been proven to provide interoperability between systems are fingerprint images.	
267	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	Fingerprint images can accommodate interoperability issuing stemming from dissimilar acquisition devices, varying image sizes, resolutions, and grayscale depths (I.e. bits per pixel). Most significantly however, it provides modular choice of the matching algorithm.	
268	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	There are different biometric fingerprint data interchange format standards available for use. Specifically, the ANSI/NIST-ITL 1-2000 (for enrollment), and the ANSI INCITS 381-2004 (for authentication) standards address the interchange of fingerprint images.	
269	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	In addition, ANSI INCITS 378-2004 defines a fingerprint minutiae template that has been developed as a more efficient alternative to image-based exchange.	
270	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	The interoperability of minutiae template data will be tested by NIST in the MINEX04 evaluation scheduled to conclude in late 2005.	
271	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	Exchange of minutiae data has been standardized by ANSI-INCITS 378-2004. This standard is substantially the same as the ISO/IEC 19794-2 currently nearing final international standard status.	
272	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	Although conformance testing standards are currently under development in INCITS M1.3, no conformance standard for minutiae is currently available.	
273	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	Pending the completion and conclusion of the MINEX04, the interchange of fingerprint image data currently provides the greatest level of interoperability between dissimilar fingerprint recognition systems.	

274	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	It provides implementers of these systems the flexibility to accommodate image captured from dissimilar devices and varying image sizes.	
275	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.2 Page 31	Where electronically submitted, fingerprint images compliant with ANSI/NIST-ITM 1-2000 shall be used for biometric enrollment as described in Section 4.4.3. Fingerprint images compliant with INCITS 381-2004 shall be stored on PIV cards for identity verification as described in Section 4.4.4.	
276	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 31	Fingerprint Requirements for Biometric Enrollment. The overall format for recording, storing, and transmitting the biometric information for PIV enrollment shall be as specified in the ANSI/NIST-ITL 1-2000 standard and the CJIS-RS-0010, Electronic Fingerprint Transmission Specification and appendices (EFTS).	
277	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 31	The captured images shall be plain impressions (also called a slap or flat) obtained from multiple fingers simultaneously placed on a platen without any rolling movement. Alternatively, a corresponding set of rolled images may accompany the plain impressions.	
278	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	Sets of the required ten fingerprints (not required to be stored on the card) shall be captured through three multi-finger images.	
279	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	a) Combined impression of the four fingers on the left hand (except for the thumb). b) Combined impression of the four fingers on the right hand (except for the thumb), and c) Combined impression of both the left and right thumbs.	
280	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	The location for each of the fingers within the overall multi-fingerprint images shall be specified within the formatted data as the left, right, top, and bottom pixel locations.	

281	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	The maximum size for the (a) and (b) images above shall be no greater than 83.3mm X 76.2mm. For the two thumbs, the maximum area shall be no greater than 50.8mm X 76.2mm.	
282	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	These images shall be referenced through codes 13, 14, and 15, to represent the left four fingers, right four finger, an two thumbs respectively.	
283	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	Table 4-6 lists all of the required fields for the Type 14 ANSI/NIST formatted record used to transmit the enrollment images to the FBI for searching.	
284	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	Additional details addressing the formatting of the data in the ANSI/NIST transaction are contained in Annex C.	
285	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	Scanning resolution used for image capture should be such that the output of the (delivered) image has a resolution of 500 pixels per inch (ppi), plus or minus 5 ppi, where each pixel represented by eight bits, or 256 grayscale levels.	
286	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	Images shall be captured by devices that have been FBI certified as compliant with Appendix F requirements of the FBI's Electronic Fingerprint Transmission Specification (EFTS/F)	
287	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	A certified version of Wavelet Scalar Quantization (WSQ) for 8-bit 500 ppi grayscale images is the acceptable image compression algorithm. Alternate compression algorithms like JPEG 2000 are not recommended since its standard specifies several versions/options and also there is no certified baseline JPEG 2000 version.	
288	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	The NIST Fingerprint Image Quality (NFIQ) method, discussed in NISTIR 7151 shall be used as the mechanisms for making an acquisition-time quality assessment that is predictive of that image's match performance.	

289	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.3 Page 32	The NIST NFIQ level must be supplied through a Finger Image Quality field in the Type-14 record. Although the un-segmented fingers shall be contained in the slap images, a unique NFIQ level must be derived and recorded for each finger of the images. this is a mandatory requirement for all slap (flat) fingerprint submissions to the FBI database starting March 2005.	
290	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.4 Page 34	Fingerprint Requirements for Identity Verification. This standard requires the capture of the fingerprint image from the left and right index fingers for the purpose of PIV card authentication.	
291	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.4 Page 34	The PIV card format requirements or the capture, recording, storing, and transmitting the biometric information for PIV authentication shall be as specified in the ANSI/INCITS 381-2004 standard.	
292	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.4 Page 34	Likewise, the compression algorithm, image resolution, and pixel depth requirements for authentication shall be the same as specified for card enrollment.	
293	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	E	FIPS201, PART 2, Section 4.4.4 Page 34	At the authentication station, two fingerprints shall be captured: (a) an impression of the left index finger and (b) an impression of the right index finger.	Remove the word "and" and (b)- duplicate.
294	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.4 Page 34	These images shall be processed and compared to the images on the card and a subsequent threshold-based decision apparatus will render a verification decision.	
295	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.4 Page 34	ANSI/INCITS 381-2004 stipulates that individual finger records be embedded within a Common Biometric Exchange File Format (CBEFF) (MISTIR 6529-2001).	
296	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.4 Page 34	The fingerprint records generated for PIV card approval will be embedded in such a CBEFF-compliant data structure.	

297	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.4 Page 34	The identification that the finger records conform to ANSI/INCITS 381-2004 should be provided in the appropriate locations in the CBEFF embedding record through the Format Owner and Format Type Code fields with values 0x001B (decimal 27) and 0x0401 (decimal 1025) respectively.	
298	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5 Page 35	Face Representation. This standard supports the use of facial images in three circumstances: Unavailable Fingerprints - When applicants are unable to present fingerprints because of disability for example, the facial image may be used. Multimodal Applications - the facial image may be used in conjunction with the fingerprint image if lower false acceptance rates are required. Visual Inspection - the electronic facial image may be used by a human inspector in a formalized process for identity verification.	
299	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5 Page 35	Facial images must comply with all normative clauses of ANSI/INCITS 385-2004. Because that standard is generic across many applications it includes clauses that have either-or requirements The following paragraphs give specific PIV requirements for such cases.	
300	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.1 Page 35	Image Type. The face record format used for PIV shall comply with all requirements of the Token Image Type defined in the Section 9 of ANSI/INCITS 385-2004. The Token specifications define geometrical properties of the face relative to the image. Particularly the center's of the subject's eyes must be located and placed at specific pixel locations. Thus PIV implementations shall locate the eyes, either automatically or manually, and rotate and translate the image to conform to the Token geometry.	
301	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.2 Page 35	Expression. The PIV card facial image shall be acquired from an applicant with a neutral facial expression.	

302	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.3 Page 35	Image Color Space. The image data shall be encoded with the YUV color space with 422 chrominance sub sampling.	
303	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.4 Page 35	Resolution. Face resolution performance is a function of the spatial resolution of the image (NISTIR 7083). Face resolution is conventionally specified by the distance, in pixels, between the centers of the subject's two eyes. The PIV card image shall have an eye-to-eye resolution of 130 pixels - the higher resolution shall be used if the PIV card has sufficient storage capacity. Images shall be acquired such that their native resolution is greater than or equal to 120 pixels from eye-to-eye. Acquisition at lower resolutions with subsequent interpolation shall not be applied. Scaling of images from larger sizes to achieve the 120 pixels specifications shall be done in one step.	
304	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.5 Page 35	Compression. Because PIV cards are likely to have limited storage space, and face recognition performance has been demonstrated to be sensitive to compression ratio (NISTIR 7083), we need to have a trade off in choosing the correct compression ratio. PIC images shall be compressed using the baseline JPEG compression algorithm using a 30 : 1 compression ratio. This provides images with required accuracy without consuming too much of storage space.	

305	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.5 Page 36	The images shall be acquired in a raw form and shall not at any intermediate stage be compressed in any way other than that mandated for final Token image. The image can be acquired from a person in a digital form using a digital camera that can generate image meeting the pixel requirements. Image acquisition systems should not apply compression before the eye-location, scaling, rotation and translation operations are performed during preparation of the Token image.	
306	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.6 Page 36	Distortion. All image acquisition systems shall follow the guidelines in Section A8 of ANSI/INCITS 385 to produce a standard radial distortion.	
307	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.4.5.7 Page 37	Background. The PIV card image shall be acquired with the subject in front of a uniform background.	Specified earlier in document that it had to be light-blue , suggest that you keep this verbiage in and get rid of the light-blue requirement, the issue is operation, not look
308	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.8 Page 37	Quality. As part of the PIV enrollment process, an automated assessment of facial image quality shall be made while the human subject is present. 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 given the following interpretation be interpreted as follows	
309	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.5.8 Page 37	Low quality values shall be reported if the face is non-frontal or rotated, is not located centrally or is cropped, if the image is blurred, over or under exposed, or is compressed in a manner inferior to that specified in this standard. In any case, quality values shall be developed and assigned such that they are ultimately indicative of true and/or false accept rates in verification or identification.	
310	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.4.5.8 Page 37	A standard for conformance of facial images to ANSI/INCITS 385 is under development.	Then why have you specified criteria for this in this documentation in the Zone description.

311	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 37	Protection of Biometrics. The mechanisms provided by the PIV card must protect biometric data in storage. Signatures on biometrics stored on the PIV card shall be formatted as a CMS external signature, as defined in (RFC 3852). The digital signature shall be computed over concatenation of the following CBEFF Elements:	
312	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 37 & 38	*CBEFF Header Version (If present); Patron Header Version; Biometric Type (If present); Record Data Type (If present); Record Purpose (If present); Record Data Quality (If present); Creation Date (If present); Creator (If present); Biometric Specific Memory Block (BSMB) Format Owner; BSMB Format Type; and BSMB.	
313	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 4.4.6 Page 38	The CMS external digital signature must contain the following elements:	Exact same data on Page 26?
314	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 38	Content shall be encoded in SignedData;	
315	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 38	Certificates and Certificate Revocation List (CRLs) shall not be included in the message;	
316	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 38	SignerInfos shall be present and include only a single SignerInfo;	
317	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 38	The SignerInfo shall:	
318	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 38	Use the issuerAndSerialNumber choice for SignerIdentifier.	

319	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 38	The authenticated attributes shall be present and include a serialnumber attribute with the FASC-N for the PIV card.	
320	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 38	Include the digital signature.	
321	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.4.6 Page 38	Additional information, such as the cardholder's name or the distinguished name in the cardholder's PKI certificates may be included in the SignerInfo authenticated attributes.	
322	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.5 Page 38	Card Reader Specifications.	
323	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.5.1 Page 38	Contact Reader Specifications. Contact readers shall conform to ISO/IEC 7816 Standards for the card-to-reader interface. These readers shall conform to the Personal Computer/SmartCard (PC/SC) Specification (PCSC) for the reader-to-host system interface.	
324	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.5.2 Page 39	Contactless Reader Specifications. Contactless card readers shall conform to ISO/IEC 14443 (ISO 14443) Standard for the card-to-reader interface.	
325	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.5.2 Page 39	In cases where these readers are connected to general purpose desktop computing systems, they shall conform to (PCSC) for the reader-to-host system interface.	
326	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.5.2 Page 39	In physical access control systems where the readers are not connected to general purpose desktop computing systems, the reader-to-host system interface is not specified in this standard.	
327	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.5.2 Page 39	This is necessary in order to allow retrofitting of PIV readers into existing physical access control systems that use a variety of nonstandard card reader communication interfaces.	

328	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 4.5.3 Page 39	PIN Pad Specifications. PIV cards may be activated through the contact interface by the cardholder using the mandatory PIN described in Section 4.1.5. Where the PIV card is used for physical access, the PIN pad shall be incorporated into the reader. Where the PIV card is used for logical access (e.g., to authenticate to a website or other server), the PIN pay may be incorporated into the reader or the PIN may be entered using the computer's keyboard.	
329	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.1 Page 40	Card Issuance and Management Subsystem	
330	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.1.1 Page 40	Registration Database. The registration Database is representative of the storage location(s) that hold PIV registration and cardholder data. This standard does not specify the type schema, or the interfaces for the registration repository. The standard does require that access to the registration repository shall be closely controlled with only authorized individuals allowed to read and/or modify contained information.	
331	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 5.1.1 Page 40	PKI Repository and OCSP Responder(s). The PIV PKI Repository and On-line Certificate Protocol (OCSP) Responder and intended to provide PIV card and key status information across agencies and organizations, to support high assurance interagency PIV interoperation.	Thought standard was NOT going to address interoperability?
332	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.1.1 Page 40	Agencies will be responsible for notifying Certificate Authority (CA) when cards or certificates are revoked. CAs shall maintain the status servers and responders needed for PIV card and certificate status checking.	

333	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.1.1 Page 40	The expiration date of the authentication certificate shall not be after the expiration date of the PIV card. If the card is revoked, the authentication certificate shall be revoked. However, an authentication certificate (and it's associated key pair) may be revoked without revoking the PIV card, and may then be replaced. A current, unexpired PIV authentication certificate on a card is proof that the card was issued and is not revoked.	
334	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.1.1 Page 40	Since the lifetime of authentication certificates is long, typically several years, a certificate revocation mechanism is necessary. Two are conventional: The CRL and the OCSP. CAs that issue PIV authentication certificates shall maintain a Lightweight directory Access Protocol (LDAP) directory server that holds the CRLs for the certificates it issues, as well as any CA certificates needed to build a path to the Federal Bridge CA.	
335	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.1.1 Page 40	Certificates shall contain the crlDistributionPoint or authorityInformationAccessPoint extensions needed to located CRLS and the authoritative OCSP responder. In addition, every CA that issued PIV authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues.	
336	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2 Page 40	Card Issuance and Management Processes. The requirements specified in this Section are in addition to the those specified in Section 2.2 (PIV I).	
337	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 5.2.1.1 Page 40	PIV Application and Approval. New Employees. An Applicant applies for an identify credential as a part of the vetting process for Federal employment. An Applicant provides two forms of identification from the list of acceptable document included in the Form 1-9, OMB No. 1115-0136, Employment Eligibility Verification to the PIV Registration Authority.	This is only for direct-hire employees, this standard is to address direct hire and contractors - where is the guidance on contractors. Contractors are not Federal Employees but have access to federal facilities and provide services for federal agencies.

338	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 5.2.1.1 Page 40 & 41	At least, one of the documents shall be a valid State or Federal Government-issued picture ID. The PIV Requesting Official shall submit the PIV request and photocopies of identify source documents for the Applicant to the PIV Authorizing Official. The PIV Authorizing Official shall approve the request and forward it together with photocopies of the identity source documents to the Registration Authority and the PIV Issuing Authority.	Once again photocopies of certain federal and or state issued picture id's may be illegal in some states or prohibited by law in certain federal agencies.
339	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.1.1 Page 41	The PIV request form shall include: Name, organization and contact information of the PIV Requesting Official; name, position including the position sensitivity level, and contact information of the applicant including address of applicant's parent organization; name, organization and contact information of the PIV Authorizing Official, name and contact information for the issuing organization, signatures of the Requesting Official and the Authorizing Official.	
340	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.1.1 Page 41	Based on the required position sensitivity level, the Applicant shall complete the appropriate background information form listed on Table 5-1.	

341	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.1.1 Page 41	The Applicant shall provide the completed background information form to the Registration Authority. In addition, the Applicant shall appear in person and provide two forms of identity source documents originally provided to the PIV Requesting Official. The Registration Authority shall visually inspect th eidentity source document and authenticate them as being acceptable. In addition, the Registration Authority shall compare the picture on the source document to the applicant to ensure the applicant is the holder of the identity source document. At this time, the Regisration Authority shall fingerprint the Applicant by collecting all of the Applicant's fingerprints as defined in Section 4.4.3. The Registration Authority shall conduct the appropriate background check as defined in Table 5-2 using the position sensitivity level from the PIV Request Form for the Applicant. Two of the applicant's fingerprints shall be securely maintaining for personalization of the Applican'ts PIV card as defined in Section 4.4.4. The Registration Authority may optionally also photograph the Applic	
342	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.1.1 Page 42	After successful completion of the appropriate background check, the Registration Authority shall securely notify the Issuing Authority that a PIV card can be issued to the Applicant.	
343	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.1.1 Page 42	The Registration Authority shall be responsible to maintain: completed and signed PIV request form, copies of the identity source documents, completed and signed background form received from the Applicant, results of the required background check, any other materials used to provide the identity of the Applicant.	
344	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 5.2.1.2 Page 42	Current Employees. A similar application and approval process shall be followed for current employees expect that background checks are not required if the results of the most recent previous checks are on-file and can be referenced in the application and verified by the Registration Authority.	The frequency of background checks should be agency-specific based on the level of sensitivity for the position in which the Applicant is holding employment.

345	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 5.2.1.3 Page 42	Overseas Foreign Workers. For citizens of foreign countries who are working for the U.S. Federal Government overseas, a similar process for application and approval must be established using a method approved by the Office of Management and Budget (OMB).	Suggest this process be developed by the U.S. Department of State, Bureau of Diplomatic Security. Official request for such guidance to be provided should come from OMB.
346	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.2 Page 42 & 43	PIV card Issuance. The Issuing Authority shall confirm the validity of the notification from the Registration Authority. The Issuing Authority shall digitally sign biometrics (facial image and two fingerprints), received from the Registration Authority, and store them on the PIV card during personalization. The Applicant may be asked to provide a PIN, or the Issuing Authority may generate a PIN on their behalf.	
347	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.2 Page 43	The Applicant may generate cryptographic key pairs and obtain the corresponding certificates at this time. Alternatively, the Applicant may be supplied with a on-time authenticator for use in subsequent certificate requests. In this case, the Applicant will generate their own key pairs at the own workstation. The identity token is initialized for the Applicant and issued. Actual issuance may occur during the initial visit to the Issuing Authority or may occur at a later date.	
348	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.2 Page 43	Simultaneously during the issuing stage, the recipient's name, the issuer identity, the card number, and possibly PKI certificate identification information are enrolled and registered with the backend database that supports the PIV system. Depending on the infrastructure design, this backend may be centralized or decentralized.	
349	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3 Page 43	Key management. PIV cards consistent with this specification may have one, two or three asymmetric private keys. To manage the associated public keys, agencies are required to issue and manage X.509 public key certificates as specified below:	

350	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.1 Page 43	Architecture. Certificate Authority (CA) that issue certificates to support PIV card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI. Self-Signed, Self-issued, and CA certificates issued by these CAs shall conform to Worksheet 1:SelfSigned Certificate Profile, Worksheet 2: Self-Issued CA Certified Profile, and Worksheet 3: Cross Certificate Profile respectively in (PROF)	
351	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2 Page 43	PKI Certificates. All certificates issued to support PIV card authentication shall be issued under the id-CommonHW policy and the id-CommonAuth policy as defined in the X.509 Certificate Policy for the Common Policy Framework (COMMON). These requirements cover identity proofing as well as the management of certification authorities (CAs) and registration authorities (RAs). CAs and RAs may be operated by agencies, or outsourced to PKI Service Providers. For a list of PKI Service Providers who have been approved to operate under (COMMON), see http://www.cio.gov/ficc/cpl.htm	
352	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2 Page 43	(COMMON) requires FIPS 140-2 Level 2 validation for the subscriber cryptomodule (i.e., the PIV). In addition, this specification requires the cardholder to authenticate to the PIV card each time it performs a private key computation with the digital signature key or key management key.	
353	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2 Page 43 & 44	(COMMON) imposes a minimum of RSA key length of 1024 bits for CA key sizes, and mandates use of SHA-1 and SHA-256 hash algorithms. CAs must use 2048 bit RSA keys when signing certificate and CRLs that expire on or after December 31, 2008. CAs that generate certificates and CRLs under this policy shall use SHA-1 or SHA-256 hash algorithm when generating digital signatures.	

354	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2 Page 44	Signatures on certificates and CRLs that are issued before January 1, 2007 shall be generated using SHA-1. Signatures on certificates and CRLs that are issued between January 1, 2007 and December 31, 2009 (inclusive) shall be generated using either SHA-1 or SHA-256. Signatures on certificates and CRLs that are issued on or after January 1, 2009 shall be generated using SHA-256.	
355	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2 Page 44	Note that additional cryptographic algorithms (e.g., ECDSA) are specified in the following text. Future enhancements to (COMMON) are expected to permit use of additional algorithms. For conformance to this specification, PIV card management systems are limited to algorithms and key sizes recognized by this standard and the current version of (COMMON)	
356	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2.1 Page 44	X.509 Certificate Contents. The required contents of X.509 certificates associated with PIV private keys are based on the X.509 Certificate and CRL Profile for the Common Policy (PROF). The relationship is described below:	
357	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2.1 Page 44	HTTP URI's required by (PROF) in the SIA, AIA, and CDP extensions are optional for this specification,	
358	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2.1 Page 44	AIA extensions shall include pointers to the appropriate OCSP status responders, using the id-ad-OCSP access method as specified in Section 8 of (PROF), in addition to the LDAP URIs required by (PROF).	
359	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2.1 Page 44	If private key computations can be performed with the PIV authentication key without user intervention (beyond that required for cryptomodule activation), the corresponding certificate must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension.	

360	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2.1 Page 44	Certificates containing the public key associated with a digital signature private key shall conform to Worksheet 5: End Entity Signature Certificate Profile in (PROF).	
361	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2.1 Page 44	Certificates containing the public key associated with a PIV authentication private key shall conform to Worksheet 5: end Entity Signature Certificate Profile in (PROF), but shall not assert the nonRepudiation bit in the keyUsage extension and must include the PIV card's FASC-N in the subject alternative name field.	
362	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2.1 Page 44	Certificates containing the public key associated with a key management private key shall conform to Worksheet 6: Key Management Certificate Profile in (PROF).	
363	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.2.1 Page 44	Requirements for algorithms and key sizes for each of these three types of PIV asymmetric keys are given in the Table 5-3.	
364	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.3 Page 45	X.509 CRL Contents. CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum. The contents of X.509 CRLs shall conform to Worksheet 4:CRL Profile in the X.509 Certificate and CRL Profile for the Common Policy (PROF).	
365	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.4 Page 45	Certificate and CRL Distribution. This specification requires distribution of CA certificates and CRLs using the LDAP. At a minimum, CA certificates and CRLs shall be distributed using LDAP. Specific requirements are found in Table II - Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements of the Shared Service Provided Repository Service Requirements (SS REP).	

366	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.4 Page 45	Considering that authentication certificates contain the FASC-N in the subject alternative name extension, these shall not be distributed via LDAP. It is an agency decision whether or not other user certificates (digital signature and key management) are distributed via LDAP. When user certificates are distributed, the requirements in Table IV - End-Entity Certificate Repository Service Requirements of (SSP REP) shall be satisfied.	
367	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.5 Page 45	OCSP Status Responders. OCSP status responders shall be implemented as a supplementary certificate status mechanism. The OCSP status responders must be updated at least as frequently as CRLs are issued. The definitive OCSP responder for each certificate shall be specified in the AIA extension as described in (PROF)	
368	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.3.6 Page 46	Migration from Legacy PKIs. Agencies who PKI has cross-certified with the Federal bridge CA (FBCA) at Medium or High may continue to assert agency specific policy OIDs through December 31, 2007. Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or is-CommonAuth policy OIDs. (Agencies may continue to assert agency specific policy OIDs in addition to the id-CommonHW and in-CommonAuth policy OIDs in certificates issued after January 1, 2008)	

369	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4 Page 46	PIV Card Maintenance. Although PIV cards may be issued by issuing authorities as per the specifications laid out in this standard, these cards may not remain valid through their expiration date. The cardholder may retire, change jobs, or be fired, invalidating a previously accurate card. The PIV System must ensure this information is distributed efficiently, both with the PIV Management infrastructure and to partied authenticating a cardholder. In this regard, procedures for PIV card maintenance must be integrated into agency procedures to ensure effective card management.	
370	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.1 Page 46	Renewal. A cardholder shall apply for renewal when a valid PIV card expires. The Issuing Authority will verify the cardholder identity against the biometric information stored on the expiring card. In the event of expired, lost, or stolen card, re-issuance procedures in Section 5.2.4.2 shall be followed.	
371	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.1 Page 46	A new facial image shall be collected and stored on the PIV card. The fingerprint from the expired PIV card may be stored on the new PIV card; note that the digital signature must be recomputed with the new FASC-N.	
372	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.1 Page 46	Since the expiration date of the PIV authentication certificate and optional digital signature certificate cannot be after the expiration date of the PIV card, a new PIV authentication key and certificate shall be generated. If the PIV card supports the optional key management key, it may be imported to the new PIV card. The expired PIV card must be collected by the registration authority and destroyed.	
373	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.1 Page 46	The Parent Organization shall verify that the employee remains in good standing and personnel records are current prior to renewing the card and associated credentials.	

374	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 5.2.4.2 Page 46	Re-Issuance. In case of re-issuance, a new personalization, including fingerprint and facial image capture, shall be conducted. The Parent Organization shall verify the employee remains in good standing and personnel records are current prior to renewing the card and associated credentials.	Conflicts with earlier statement, saying that the images can be re-used. (look in vetting process section)
375	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.2 Page 46	A cardholder shall apply for re-issuance when the PIV card is expired, compromised, lost, or stolen. The cardholder can also apply for re-issuance of a valid PIV card in the event of an employee status or attribute change or if one or more logical credentials have been compromised. A re-issuance of the electronic information and cryptographic keys on the card may also be necessary if the contents of the card are locked due to the usage of an invalid PIN. However, PIN resets may be performed by well laid out and documented procedures by each individual agency.	
376	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.2 Page 47	When these events are reported, normal operational procedures must be in place to ensure that: The PIV card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status.	
377	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.2 Page 47	The PIV Certificate Issuer shall be informed and the certificate corresponding to PIV authentication key on the PIV card must be revoked. Agencies may revoke certificates corresponding to the optional digital signature and key management keys. CRLs issued shall include the appropriate certificate serial numbers.	
378	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.2 Page 47	OCSP Responders shall be updated so that queries with respect to certificates on the PIV card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records.)	

379	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.2 Page 47	For attributes changes, the Registration Authority must verify the reason for the change and keep a copy for records.	
380	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.2 Page 47	Where possible, the PIV card shall be collected and destroyed. Where the card cannot be collected, normal operational procedures shall complete within 18 hours of notification. In some cases, 18 hours is an unacceptable delay. For example, an agency may discover a cardholder's true identity is a person on a terrorist watch list. In such a case, emergency procedures must be executed to disseminate this information as rapidly as possible. Agencies are required to have procedures in place to update all servers in one hour in the case of such an emergency.	
381	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.3 Page 47	PIV Update. For a special case, where a position sensitivity level is increased, the PIV card may be updated rather than replaced. Update processes shall include: Update position sensitivity level in the CHUID, Recompute the CHUID digital signature, and store the signed CHUID on the PIV card.	
382	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.4.3 Page 47	The applicant's identity shall be re-verified as in the case of PIV renewal (Section 5.2.4.1) The Issuing Authority shall verify Applicant's new position sensitivity level and completion of identity proofing requirements before updating the PIV card.	
383	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.5 Page 47	PIV Card Termination. The termination process is used to permanently destroy or invalidate the usage of the card including the data on it including the keys such that it cannot be used again.	

384	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.5 Page 47 & 48	The PIV card shall be terminated under the following circumstances. An employee separates (voluntarily or involuntarily) from Federal Service; an employee separates (voluntarily or involuntarily) from the Federal contractor. A contractor changes positions and no longer needs access to Federal buildings or systems; A cardholder is determined to hold a fraudulent identity, or the cardholder passes away.	
385	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 5.2.5 Page 48	Similar to the situation I nwhic the card or a credential is compromised, normal termination procedures must be in place as to ensure that: the PIV card is collected and destroyed, the PIV card itself is revoked, any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status. The PIV certificate Issuer shall be informed and the certificate corresponding to PIV authentication key on the PIV card must be revoked. Agencies may revoke certificates corresponding to the optional digital signature and key management keys. CRLs issued shall include the appropriate certificate serial numbers. OCSP Responders shal lbe updated so that queries with respoect to certificates on the PIV card are answered appropriately. This may be performed indirectly (by publishing the CRl above) or directly (by updating the OCSP server's internal revocation records.)	

386	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651		FIPS201, PART 2, Section 6 Page 49	PIV Card Authentication. This information Section discusses authentication mechanisms that are supported by the PIV card and the credentials is hosts. Within the context of the PIV card, identity authentication is defined as the process of establishing confidence in the identity of the cardholder presenting a PIV card. The authenticated identity of the cardholder can then be used by an agency to make an access decision (to controlled Federal Resources) based on the agency's own authorization mechanisms and local access control policy. Thus, this Section should be treated as Informative.	This section must be prescriptive. HSPD-12 requires identity authentication before entry to a government facility. Physical access to each facility is determined by the local access control policy; therefore, this section should provide general guidelines for access screening.
387	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6 Page 49	This Section also discusses the use of the PIV card authentication mechanisms for support for physical and logical access control systems. It may be noted that the scope of this standard extends to providing a number of authentication mechanisms in "support" of agency defined access control and authroization policies. Nothing in this standard should be interpreted as a prescirptive in terms of the authroization checks and access control policies implemented by a Federal agency.	
388	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1 Page 49	PIV Card Authentication Mechanisms. The fundamental purpose of the PIV card is to serve as a means of authenticating the identity of the PIV cardholder for access to Federal resources. Thus, the PIV card supports ientity authentication in environments that are equipped with card readers as well as environments that are without card readers. In environments where the access control point is not equipped with suitable PIV card readers, visual authentication is usually performed.	

389	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1 Page 49	The PIV card may also be used in an access control environment where PIV card readers are available. In this case, electronic authentication of the cardholder may be conducted using the PIV card. Card readers may be contactless or contact-based. Contactless card readers are used to support contactless authentication of the PIV card. For privacy reason contactless use of Pins and biometrics is not supported PINs and biometrics may be used with the PIV card using contact readers.	
390	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1 Page 49	In the following subsections, various type of authentication mechanisms that may be supported by the PIV card are discussed. It is important to note that these are authentication mechanisms that are available as options to agency resource owners as they implement access control systems for protecting their resources. This standard provided descriptions of these mechanisms to assist in the implementation of authentication mechanisms for controlling access to Federal resources. It should also be noted that agencies can implement compound authentication mechanisms by using the basic authentication mechanisms specified in this Section.	
391	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 49	Authentication using PIV Visual Credentials. Visual authentication of a PIV cardholder is essential in environments where electronic verification infrastructures are either not installed, or temporary unavailable (due to network outages and system malfunction). Visual identify authentication may be used to support access control to physical facilities and resources. however, since a human verifier is needed to implement visual identity verification, this type of verification should not be used to support access to logical resources.	

392	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 50	The PIV card has a number of mandatory topographical features (in the front and back), that support visual identification and authentication, namely: photograph; name; employee affiliation employment identifier; expiration date; agency card serial number (back of card); issuer identification (back of card). The PIV card may also bear the following optional components: Agency name and/or department; agency seal; PIV card holder's physical characteristics; signature.	
393	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 50	When a PIV cardholder attempts to pass through an access control point for a Federally controlled resource facility, a human guard can perform visual identification and authentication of the cardholder, and determine whether the identified individual should be allowed through the control point. The series of steps that may be applied n the visual authentication process are as follows:	
394	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 50	1) The human guard at the access control entry point determines whether the PIV card appears to be genuine and has not been tampered with in any way.	
395	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 50	2) The guard compares the cardholder's facial features with the picture on the card to check that they match.	
396	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 50	3) The expiration date on the card is checked to ensure that the card has not expired.	
397	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 50	4) The cardholder's physical characteristics descriptions are compared to those of the cardholder (OPTIONAL0	
398	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 50	5) The cardholder's signature is collected and compared with the signature on the card. (OPTIONAL)	

399	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.1 Page 50	6) One or more of the other data elements on the card (e.g., Name, employee Affiliation, Employment Identifier, Agency Card Serial Number, Issued Identification, and Agency Name) are used to determine whether access should be granted to the cardholder.	
400	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	Authentication using the PIV CHUID. The PIV card provides a mandatory cardholder Unique Identifier (CHUID) container that is an Elementary File (EF). The CHUID data model comprises a number of data elements as described in Section 4.2.	
401	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	In environments that support electronic interaction with the PIV card, simplistic authentication mechanisms may be implemented, using the data elements contained within the CHUID. In this type of authentication mechanism, there is no attempt to correlate the data and identifies on the card with the actual cardholder. It is assumed that he cardholder is the owner of the card, and the identifiers read from the card are passed on to the access control module. Since CHUID-based authentication mechanisms are inherently weak, they may be suitable for certain physical access control environments; however, these mechanism are not recommended for logical access control systems.	
402	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	The CHUID data elements may be used for authentication sequence as follows:	
403	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	1) The CHUID is read from the PIV card.	
404	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	2) The digital signature on the CHUID is checked to ensure CHUID is intact and comes from a trusted source (OPTIONAL)	

405	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	3) The expiration date on the card is checked to ensure that the card has not expired. (OPTIONAL)	
406	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	4) One or more of the CHUID data elements (FASC-N, Agency Code, DUNS, Position Sensitivity) are used as input to the authorization check to determine whether the cardholder should be granted access.	
407	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 6.1.2 Page 51	A specific variant of the above sequence is described in the Physical Access Control System (PACS) LOW assurance profile. This is described in detail in (PACS). Another variant of the CHUID-based authentication that may be used comprises of the following steps.	The LOW assurance profile as outlined in PACS violates the precepts of HSPD-12 3(b) and (c).
408	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	1) The CHUID and the Card Unique ID (CUID) are read from the PIV card.	
409	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	2) The digital signature on the CHUID is checked to ensure CHUID is intact and comes from a trusted source (OPTIONAL)	
410	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	3) The Expiration date is checked to ensure that the card has not expired (OPTIONAL)	
411	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 6.1.2 Page 51	4) One or more of the CHUID data elements as well as the CUID are passed through a unidirectional cryptographic transform that uses a sit-specific key, such as a hashed message authentication code algorithm. The result of the cryptographic transform and CHUID and CUID elements are passed as input to the authorization function.	The MEDIUM assurance profile as outlined in PACS violates the precepts of HSPD-12 3(b) and (c). The standard's requirement for a medium assurance level with its signed CHUID does not protect the card from counterfeiting as required by HSPD-12. Only a high assurance profile provides this protection.
412	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.2 Page 51	The above authentication mechanism is aligned with the Physical Access Control System (PACS) medium assurance profile, described in detail in (PACS)	

413	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	Authentication using PIV Biometric Credentials. In environments where the collection of a PIN and a biometric sample from the cardholder is feasible a strong authentication mechanism that ties the cardholder to the card itself may be implemented. Depending upon the rigor of the checks that are used during the authentication process, this type of mechanism can be applied to logical as well as physical access control systems.	
414	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	The PIV card hosts a signed biometric that can be read from the card after the cardholder provides a PIN to perform CTC authentication. The signed biometric may be used to support and authentication mechanism through a match-off-card scheme as follows:	
415	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	1) The cardholder is prompted to submit a PIN, activating the PIV card and allowing the signed biometric to be read from the card.	
416	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	2) The signed biometric is read from the PIV card.	
417	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	3) The signature on the biometric is verified that the biometric is intact and comes from trusted source. (OPTIONAL)	
418	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	4) The cardholder is prompted to submit a live biometric sample.	
419	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	5) If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.	
420	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	6) The CHUID is then read from the card.	

421	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	7) The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.	
422	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	8) The Expiration date in the CHUID is checked to ensure that the card had not expired (OPTIONAL)	
423	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.3 Page 52	9) One or more of the CHUID data elements (FASC-N, Agency Code, DUNS, Position Sensitivity) are used as input to the authorization check to determine whether the cardholder should be granted access.	
424	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.4 Page 52	Authentication Using PIV Symmetric Cryptography. The PIV card may optionally support the PACS compliant symmetric key cryptographic data model and functions. The PACS site-specific symmetric key is stored a PIV local authentication key as defined in Section 4.3. The PIV card supports PACS compliant challenge-response based authentication schemes that use symmetric cryptography, as in the following sequence:	
425	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.4 Page 52	1) The CHUID is read from the card.	
426	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.4 Page 53	2) The Expiration date in the CHUID is checked to ensure that the card had not expired (OPTIONAL)	
427	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.4 Page 53	3) The reader issues a challenge string to the card request a symmetric operation in response.	
428	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.4 Page 53	4) The response received from the card is compared with a parallel computation using sleeted data elements from the CHUID, along with a site-specific symmetric key to check that they match.	

429	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.4 Page 53	5) The CHUID elements are passed as input to the authorization function.	
430	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.4 Page 53	The above authentication mechanism is aligned with the Physical Access Control System (PACS) high assurance profile, described in detail in (PACS)	
431	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.5 Page 53	Authentication using PIV Asymmetric Cryptography. In access control environments where asymmetric cryptographic capabilities are available, the PIV card may be used to perform identity authentication using asymmetric key mechanisms. The PIV card carries a mandatory asymmetric authentication private key and corresponding certificate, as described in Section 4.3 the PIV card can support an asymmetric authentication mechanism comprising the following steps:	
432	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.5 Page 53	1) The reader issues a challenge string to the card and requests an asymmetric operation in response.	
433	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.5 Page 53	2) The cardholder presents their PIN or biometric sample. The authentication information is submitted to the card, is verified, and the card is activated.	
434	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.5 Page 53	3) The card responds to the challenge by signing it suing the authentication private key, and attaching the associated certificate.	
435	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.5 Page 53	4) The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to be from a trusted source.	
436	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.5 Page 53	5) The response is validated as the expected response to the issued challenge.	
437	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.1.5 Page 53	6) The Subject DN or FASC-N from the authentication certificate is extracted and passed as input to the authorization function.	

438	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.2 Page 53	Authentication for Physical Access Control. The PIV card can be used to authenticate the cardholder in a physical access control environment. For example, a Federal facility may have physical entry doors that have human guards at checkpoints, or have electronic access control points.	
439	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 6.2 Page 53	PIV cards can be used for physical access control in a visual, contactless or a contact-based environment. Visual authentication may be used alone or to supplement a contactless or contact-based authentication process.	Visual authentication can not be used as a mechanism as it is not electronic and provides no assurance of identity validation. Although, the Directive calls for a least secure to most secure graduated criteria, even the least secure must meet the directives objectives, visual authentication is not in compliance with the Directive.
440	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 6.2 Page 54	Within a contactless environment, the card is able to get power for a very brief period and can only participate in a very rapid authenticating dialogue with the reader. Additionally, contactless cards/readers are usually deployed in high volume usage environments where rapid authorization decisions need to be made. Hence, implementations that require complex computational operations or lengthy backend verification processes are typically less suitable for the contactless environment.	As a physical access control mechanism, the proposed use of contactless is not rapid, is not electronic, and is not identity authentication.
441	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.2 Page 54	For contact-based physical access control, the card is able to draw power directly from the card reader and can hence participate in more complex protocol intercahnges with the reader. Additionally, these mechanisms make use of cardholder PIN or biometric.	
442	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.2.1 Page 54	Assumptions and Constraints. The physical access environment typically has the following characteristics:	
443	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.2.1 Page 54	The environment may need to support a medium to high volume of entry, which implies that the time required for authenticating a single cardholder has to be very short.	

444	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.2.1 Page 54	Physical access control points are typically not connected to an agency's logical network or the Internet. Hence mechanisms that rely upon online key management techniques or status lookups are not practical.	
445	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.2.1 Page 54	Thus, typical electronic physical access control systems are standalone in nature, and implement local authorization decisions, without the ability to access networked infrasturcture services that provide verfication or status information.	
446	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 6.2.1 Page 54	Another implication of this standalone environment is that it is infeasible to implement online key management mechanisms for establishing authentication keys between the PIV card and the secure site. Thus, physical access control systems tend to rely heavily upon offline or out-of-band means of pre-approving a cardholder for access to a particular secure site, and on the use of offline key management processes to obtain site-specific authentication key that is injected into a PIV card to allow access to a particular secure site. As a result, physical access control systems are not typically able to support the scenario where a PIV cardholder can be authenticated in real-time to as secure site to which his access has not been pre-approved and pre-configured.	It should be understood that the cardholder should have no expectations of gaining physical access to a facility based on the fact that they are a valid PIV card holder. The purpose of the card is identity assurance - no access assurance.
447	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.2.2 Page 54	Applicable Authentication Mechanisms. Some PIV-supported authentication mechanisms for physical access control systems are described below.	
448	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.2.2 Page 54	Each of the authentication mechanisms described below can be further strengthened through the use of a backend certificate status verification infrastructure. Federal applications may augment authentication mechanisms for physical access control through the use of revocation status providers for the PIV card authentication certificate.	

449	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.3 Page 55	Authentication for Logical Access Control. The PIV card may be used to authenticate the cardholder n support of access control decisions for information resources. For example, a cardholder may login to their agency network using the PIV card. The identity established through this authentication process can be used for determining access to file systems, databases, and other services available on the network.	
450	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.3 Page 55	Assumptions and Constraints. The logical access environment is characterized by the following attributes:	
451	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.3 Page 55	An untrusted network connects the PIV cardholder and the information resource.	
452	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.3 Page 55	Logical access control points usually have sufficient network access to support the use of online key management schemes and online status lookups during the autehntication process.	
453	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE		FIPS201, PART 2, Section 6.3 Page 55	Contact interface is preferred for logical access control.	Recommend that use of contact cards be required until the establishment of contactless card technology can fully support symmetric keys.
454	U.S. DEPARTMENT OF STATE			FIPS201, PART 2, Section 6.3 Page 55	Thus, typical logical access control systems are connected to networks of other systems and resources, have contact-based card readers, and have the ability to access networked infrastructure services that provide verification or status information. Logical access control environments can also support the implementation of online key management mechanisms for establishing authentication keys between the PIV card and secure site.	