Submitted by: U.S. Department of State, Bureau of Diplomatic Security
Date: December 10, 2004

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		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.	We believe that copies of the original documents must be digital copies and stored at a secure website or some other location that is accessible by remote ID card units. DoS and other agencies are required to re-issue lost ID cards and issue ID cards to new employees. The documents used to authenticate the employee's identity must be available to all ID card issuers in that agency.
2	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	FIPS201, PART I, Section 2 Page 4	PIV-I addresses the fundamental control objectives and security objectives outlines in HSPD-12, including the personal identity proofing process for new employees, but does not address interoperability of PIV cards and systems among agencies or compel the use of a single, universal credential.	There is no specific requirement in the HSPD-12 for Interoperability, DoS supports interoperability at the high assurance profile level.
7	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	FIPS201, PART I, Section 2.1 Page 4	Issue credentials through systems and providers whose reliability has been established by the agency and so documented and approved in writing:	The next 3 lines are directly from the HSPD-12, but are out of order, suggest you align them properly and use the wording exactly as it is in HSPD, do not attempt to expand the PD. Use specific PD references I.e (3a, 3b, 3c, 3d)
8	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	FIPS201, PART I, Section 2.1 Page 4	Issue identity credentials that are resistant to identify fraud, tampering, counterfeiting, and terrorist exploitation;	See Above
9	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	FIPS201, PART I, Section 2.1 Page 4	Implement an identify credentialing system that supports repid electronic authentication of Federal employees and contractors, and	See Above

D = Document, 1 = FIPS201, 2= SP800-73
T=Type of Comment, E = Editorial, T = Technical

10	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**G**	FIPS201, PART I, Section 2.1 Page 4	Support credentials for physical and logical access to Federally controlled facilities and information systems.	This line does not belong in PIV I, move to PIV II.
11	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**G**	FIPS201, PART I, Section 2.1 Page 4	In PIV-II these identity proofing and issuance requirements are maintain, and a common government-wide, interoperable PIV card is required.	Suggest you use the term PIV Credential v. Card.
12	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**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 or implied that simply having the card entitles any employee physical or logical access to a facility or system.
13	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**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 registration process defined in Sections 2.2.1 - 2.2.4 when issuing identify credentials.	You refer to the control objective by number, yet they are not numbered in the document. Suggest you number the control objectives so as to avoid confusion.
14	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**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 can work in the Domestic world, but overseas it is definitely going to be a problem. To allow for overseas use suggest that you change the word "Shall" to "Should"
17	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**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;	Suggest you add the word authorized before the word individual.
18	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**G**	FIPS201, PART I, Section 2.2 Page 5	PIV Authorizing Offical - The individual who approves the request for an identiy credential;	Suggest you add the word authorized before the word individual.
19	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**G**	FIPS201, PART I, Section 2.2 Page 5	PIV Regisration Authority - The entity that perform the identity proofing and background checks;	The word Regisration is so widely used in the PKI world that it becomes confusing when used in this context. Suggest you change this title to PIV Adjudication Authority - this will make it clear and consise to both logical and physical security personnel.

20	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	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.	Suggest you add the word authorized before the word entity.
21	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	FIPS201, PART I, Section 2.2.1 Page 5	The paper-based source documents by themselves provide very weak assurance of identity.	Take out the word "the" at the beginning of sentence.
26	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	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.	Suggest adding the option of "or digitally signed electronic equivalent" after the word photocopies. (The paperwork reduction act should be considered as it appears that multiple copies of this information must be maintained by several different Officials, one electronic copy would be more efficient and comply with the paperwork reduction act)
27	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	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	Cynthia Atkinson DS/ST/FSE	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;	Might want to add some verbiage as to who is an authorized Requesting Official, it is only HR personnel, Government Employees, Supervisors etc. Without such clarification we could end up with Contractors requesting badges for other contractors.
30	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	FIPS201, PART I, Section 2.2.1 Page 5	Name, organization, and contact information of the PIV Authorizing Official;	Once again, clarification as to who is an "Authorizing Official", must be government employee etc.
33	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	FIPS201, PART I, Section 2.2.1 Page 5	Signatures of the Requesting and the Authorizing Officials.	If the paperwork is done electronically after the hard copy identity proofing process is completed can these be digital signatures?

37	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	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.	Issue 1: Once again, strongly urge the use of the term "Adjudication Authority" vs Registration Authority. Issue 2: You state that this person who authenticates the documents will do this based on a visual inspection of the document? Without access to multiple databases, how can they be expected to truly validate that the identification document is true and valid. Recommendation: Require electronic validation in addition to a visual inspection to truly validate submitted documents.
40	U.S. DEPARTMENT OF STATE	Gary Schenk GLID Program Manager	G	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.	Must this be done by the Registration Authority? Can it be performed by a different Authority in the process?
41	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	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....
43	U.S. DEPARTMENT OF STATE	Gary Schenk GLID Program Manager	G	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, takes fingerprints, and performs background checks which are the Registration Authority's responsibility.
48	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	FIPS201, PART I, Section 2.2.1 Page 7	Copies of the identity source documents;	Again one copy, digitally stored and available to authorized officials in the ID card authentication process should be the requirement.

52	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE Gary Schenk GLID Program Manager	**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. Additionally the expired PIV card must be returned before a new card can be issued.
54	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	**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.	At this time we have not received any form of request or notification from OMB that we need to establish and provide such process documentation. Request formal notification from OMB of this requirement.
55	U.S. DEPARTMENT OF STATE	Gary Schenk GLID Program Manager	**G**	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.	What is the process of validation of the PIV request?
58	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE Gary Schenk GLID Program Manager	**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.	Do not specify where in the process the photograph is obtained.
60	U.S. DEPARTMENT OF STATE	Gary Schenk GLID Program Manager	**G**	FIPS201, PART I, Section 2.3 Page 7	The Issuing Authority shall be responsible to maintain: Completed and formally authorized PIV Request.	Also, should keep something from the Adjudication Authority that the background checks completed ok.
61	U.S. DEPARTMENT OF STATE	Gary Schenk GLID Program Manager	**E**	FIPS201, PART I, Section Section 2.3 Page 7	The name of the PIV identity credential holder (Applicant).	Suggest reword to: The name of the credential holder (applicant).

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	This Standard does not require electronic cardholder authentication as required by HSPD-12. Nothing less than the High Assurance Profile techniques protect the PIV card from counterfeiting and cloning as mandated by the directive. The graduated criteria required in the directive must provide PIV (card to card-holder) authentications within the high assurance profile.
16	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	FIPS201, PART 2, Section 3.1 Page 10	Protect the privacy of the cardholder,	NOTE: The privacy of the cardholder requires encryption of personal data.
17	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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;	The interface must be flexible. Currently, file container and Java cards are being used; however, IP addressable cards will soon be available and other types of cards will follow. The interface must be flexible to ensure that the government can quickly move to higher security cards, while minimizing the cost on infrastructure upgrades.
18	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	FIPS201, PART 2, Section 3.1 Page 11	Provide appropriate security to the entire identity proofing and authentication process;	The appropriate security for the DoS is the high assurance security.
19	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	FIPS201, PART 2, Section 3.1 Page 11	Provide protection against use of cloned or counterfeited PIV cards;	Use high assurance only

21	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	This is a core issue for DoS. DoS will require high assurance for the PIV data security. The minimum requirement for interoperability must be the high assurance level in order to protect the personal information contained on the card. This is critical to the Foreign Afairs agencies operating in the diplomatic overseas enviornment. If the data is not protected at the high assurance levels, DoS will require an exemption for over seas use under 44 U.S.C. 3542(b)(2). Other agencies may use lower levels of assurance for internal operations, but must provide high assurance for interoperability with DoS.
29	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.
35	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.
85	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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	G	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	G	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).
94	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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 and should not be required.
108	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.

110	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.
114	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.	Delete this requirement. It does not reduce conterfeiting nor improve cardholder identity.
115	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.	Suggest the format of MM/YY and a minimum of [18 to 22] pt. Delete the requirement for the word "expires".
116	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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 the diagrams below are not to scale.	There should be no mandatory information on the back of the card except for Geneva Convention and Return to information.
117	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	Suggest that this be titled the Credential Serial Number and should be printed on the front of the card.
118	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	This number should not be printed on the card. The data should be recorded on the smart chip and used in the electronic authentication of the card.

127	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	Indicate that this is optional as per figure 4.1. If this is not intended to be optional and figure 4.1 is incorrect, issue date is irrelevant recommend this be deleted or made optional.
129	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	The magnetic stripe should be mandatory for all cards. Many agencies use mag. stripe for internal physical access in legacy systems. Having a mag. Stripe on the card will provide a good business case by allowing one card to be used for interoperability, physical access and logical access. Adjust in Figure 4.1 as well.
131	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	Indicate that this is optional as per figure 4.2. If this is not intended to be optional and figure 4.2 is incorrect, physical characteristics are irrelevant recommend this be deleted or made optional.
132	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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."	Emergency responder data (if used) should be on the front of the card. Indicate that this is optional as per figure 4.2.
142	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.

145	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	This is a core issue for DoS. DoS will require high assurance for the PIV data security. The minimum requirement for interoperability must be the high assurance level in order to protect the personal information contained on the card. This is critical to the Foreign Affairs agencies operating in the diplomatic overseas enviornment. If the data is not protected at the high assurance levels, DoS may require an exemption for over seas use under 44 U.S.C. 3542(b)(2). Other agencies may use lower levels of assurance for internal operations, but must provide high assurance for interoperability with DoS.
159	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	T	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.
176	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	E	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
184	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.	DoS has 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 meets the directives objective.

185	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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 meet the directive.
186	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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 meet the directive.
187	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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 meet the directive.
188	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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 meet the directive.
189	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.
207	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	T	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.
247	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.
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.
307	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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
310	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.

313	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	E	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?
337	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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	G	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.
344	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.
374	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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)

386	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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 agency's access control policy; therefore, this section must provide minimum requirements for individual authentication prior to entering the facility. If the facility has an access control system that can electronically authenticate the individual and card, this method should be used for all authorized personnel and this section should provide the guidelines for this process. Visitors would undergo the same process at a visitor station that is connected to the interagency network. Agency access control networks will be controlled by the parent agency, but when authorized, individuals from other agencies should be able to have their PIV entered into the access control system and use their PIV for access control at that federal facility.
388	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	This is a core issue for HSPD-12. The present system provides for visual authentication. Please explain how issuing a smart card with the same visual data that is on present ID cards is any more secure than legacy ID card systems. We believe that the reason for HSPD-12 stating a requirement for rapid electronic authentication is that it must be used. The exception would be for small facilities where a guard can be expected to personally recognize all of the employees.

389	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	This statement must be prescriptive. Electronic authentication must be a requirement at the high assurance profile.
391	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	This statement should not mix physical and logical access. Visual authentication by a person is acceptible if that person can be reasonably expected to know all of the employees in that facility. Otherwise, electronic authentication will be a requirement. Delete the last sentence on logical access.

392	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	Mandatory topographical features must be on the front of the card where the guard can see the data. Throughput to the facility will decrease if the guard has to ask the employee to remove the card from the holder (no holes in the card so there must be a card holder). The agency card serial number and issuer identification data is useless to the guard. The guard will neither have a list of valid serial numbers nor a list of list of issuer identification numbers. The guard looks at two items of data. The picture and the expiration date of the card. Again, visual authentication must be restricted to facilities where the guard can be expected to recognize all employees.
393	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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:	You need to reassess this section. Agencies use this process now. What is the business case to change to a smart card that can provide electronic authentication and physical access control without using the capability? If the agency can't answer the question positively, they should stay with the legacy system or convert to electronic authentication.
397	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	E	FIPS201, PART 2, Section 6.1.1 Page 50	4) The cardholder's physical characteristics descriptions are compared to those of the cardholder (OPTIONAL0	Typo change to (OPTIONAL)
399	U.S. DEPARTMENT OF STATE	Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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.	Employee identifier, Agency serial number, and issued identification are useless in visual authentication.

407	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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). Low assurance must not be used as the minimum requriement.
411	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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. Medium assurance must not be used as a minimum requirement.
439	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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 except at facilities where a guard can be expected to recognize the individuals who work there. 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 Walter G. Felt Chair, FSE TWG DS/ST/FSE 703/923-6651	G	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 secure, and it does not provide identity authentication.

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.
453	U.S. DEPARTMENT OF STATE	Cynthia Atkinson DS/ST/FSE	G	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.