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.	