Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
1	DoD		G		The technical framework presented by National Institute of Standards and Technology (NIST) breaks the existing credentialing systems of the Department of Defense (DoD) and other Federal Agency systems that currently support the existing NISTR 6887 smart card specification. All the Federal partners are aware of the ambiguities in the current specification, but have worked with NIST via the Federal Interagency Advisory Board (IAB) to promote changes and tighten the specification over the past three years. NIST has the option to tighten the current specification or to propose a whole new standard.	
2	DoD		G		The preliminary draft of FIPS 201 is a new specification that has not been implemented by any government agency or vendor. The vendor community has provided products that support the current DoD implementation (e.g. Blackberry, smart card and integrated circuit (IC) vendors, middleware vendors, physical security companies, biometric vendors, etc). FIPS 201 will require all agencies and vendor products that currently support NISTR 6887 to change infrastructure, retool software, recertify applications and processes, and place the new Personal Identity Verification (PIV) framework on the cards of their members. Currently, DoD, Department of Homeland Security (DHS), Department of Interior (DOI), National Aeronautics and Space Administration (NASA), and Department of Veterans Affairs (VA) are implementing NISTR 6887 compliant card systems. These organizations represent approximately 85% of the Federal target population.	
	DoD		G			

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
3	DoD		G		The vendor community has been forthcoming in supporting NISTR 6887. Many companies have invested large sums of research and development dollars into developing compliant products in support of their government customers. There is a risk that these companies will be unwilling to reinvest to be compliant with another standard that is untested with no guarantee of adoption. It was assumed that the draft PIV effort would use the foundation of NISTR 6887 as its core. This has not been the case, and it will require DoD to modify their issuance system, revise and redeploy desktop middleware to 2.2 million DoD computers, and update the Common Access Cards (CAC) of 3.5 million DoD personnel. This effort will be resource intensive and delay the deployment of new capabilities to our identity protection and management initiative (e.g. post issuance capabilities). For DoD, this will be a four to five year effort. Other first adopters in the Federal government of NISTR 6887 are at various points in their implementations, but all will have to retool and reissue cards to be compliant with HSPD 12 if the current FIPS 20	
4			G		The business viewpoint is clear. Federal agencies representing approximately 85% of the target HSPD-12 population that support the current NIST specification (GSC-IS v2.1) will have to retool and reissue. DoD will take the longest to achieve compliance, and current estimates say it will take 4-5 years. The reaming 15% of the population will be able to implement PIV when it becomes available. Given the above considerations, DoD is not confident that implementation of PIV will commence within the mandated HSPD-12 timeline.	

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
5			G		Instead of moving forward with NISTR 6887 and rapidly achieving HSPD-12 compliance in the Federal government, the current PIV Standard will impose an unproven solution with no supporting product on **100%** of the Federal population. The DoD CIOs and program managers will be hard pressed to explain and defend this decision to their senior leadership	
6	DoD		G		Department of Defense already has a strong, secure credentialing program in place that cannot technically, physically, or economically be discarded and replaced in a matter of months. Over-engineering the interoperable Federal credential solution would potentially result in DoD replacing their entire architecture, and it would not provide the flexibility that the Federal government will require.	All Federal programs issuing smart ID cards should be grandfathered into a minimum acceptance level of FIPS 201. There must be a clear migration plan that takes existing technology into account but also provides firm direction (both technically and in policy) to promote federal interoperability.
7	DoD		G		The Draft of NIST FIPS 201 requires that a member have an authentication level placed on their card that defines a level of trustworthiness. For DoD personnel (civilian, military and contract support personnel) who operate in adverse environments and may be subject to capture, this could easily be an indicator of the level of information a person may be able to access and a potential measure of the individual's importance. This draft requirement will subject DoD personnel to unnecessary risk and does not take into account Geneva Convention requirements. In the implementation of the CAC, we have taken great care to balance Geneva Convention requirements by keeping the CAC a pure statement of identity, while placing the level of access on the network, reliant-parties, and separate clearance systems.	

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
8	DoD		G		There are significant operational risks associated with implementing the PIV standard. The DoD relies on the CAC and PKI to protect information and information systems. PKI policy requires use of the CAC to digitally sign email, mutually authenticate to web sites, and cryptographically authenticate to networks. Implementing a new CAC and PKI structure will likely degrade the reliability, availability and performance of the current infrastructure. This would have significant adverse impact on DoD operations.	
9	DoD		T	Section 5.2	The Standard requires a PIV requesting official and a PIV authorizing official.	The issues that need to be addressed include: the standards for each of these positions; the training and certification of these individuals; and the certification level, which dictates the level of sensitivity vetting for the applicant. For example, a level 4 authorizing official is the only qualified official to authorize level 4 applicants.
10	DoD		T	Section 5.2.3	Is the backend database that supports the PIV system the same as the PIV card management system (sec 6.6)?	Be consistent when referring to the various backend databases.
11	DoD		T	Section 5.2.4.3	PIV renewal	Need to define the life cycle requirements, for example, the maintenance process in the PIV database.
12	DoD		T		Employee's change of status is missing from the standard.	PIV system must be able to handle the change in status of an employee with respect to the token between issuance. For example, an employee dies, where is the card termination and employee information removed or flagged in the PIV backend databases?

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
13	DoD		G		Privacy protection	Standard must address the privacy implications of the data being requested and used for matching. Please reference Privacy Act of 1974. Also, need to make sure that current regulations allow Registration Authority to maintain a completed and signed background form and the results of the required background check..
14	DoD		T		The Geneva Accord provides Geneva Convention Protection to military members, medical personnel, religious personnel, and civilians authorized to accompany the military forces into areas of combat. To comply with the Geneva Accord, certain information is required to be displayed on the DoD credential. To meet this requirement, the back of the proposed card for military members should be for all DoD personnel to include both military and civilian personnel.	To meet this requirement, the back of the proposed card for military members should be consistent with the cards for all DoD personnel to include both military and civilian personnel.
15	DoD		T	Figure 4-1	Zones 8,9,10	Placement of zones 8 and10, as well as requiring zone 9 will cause current DoD cards to be non-compliant.
16	DoD		T	Figure 4-1	Zone 13 – Issue Date is Optional	Consider making this field mandatory.
17	DoD		T		The Green and Red stripes are no longer part of the front of the card. There are no provisions for identifying Foreign Nationals.	Provide consistent federal guidance in policy or modify topology.
18	DoD		T	Figure 4-3	On the back of the Military PIV Card, the current control number is printed above the magnetic stripe not under the bar code.	Make the location of the Control Number optional.
19	DoD		T			Include Escrow and Recovery of Key Encipherment Keys to the list of lifecycle activities, at least optionally.
20	DoD		G		Paper documents should be reduced.	To support the Paperwork Reduction Act, FIPS 201 needs to require use of digital documents.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
21	DoD		T		PIV issuer has major systems to maintain: 1) PIV card management system2) PKI certificate management system3) Interfaces to parent organization database and OCSP databases	All three systems are resource intensive activities. Additionally, this process does not allow for the same checks and balances in the PIV registration process with the PIV issuance process:because all data control is moved to one central responsible official.
22	DoD		T		The standard does not address how organizations should evolve their security posture with respect to the physical card, such as technical advancements that improve anti-counterfeiting measures.	The standard should provide for a 3 year life cycle for any single physical technology. This would require card issuers to change the security features of their cards regularly.
23	DoD		T		Cryptographic key storage is not specified.	This could lead to possible interagency discrepancies where one agency stores the cryptographic keys very securely while another one does not. This weakens the overall Federal initiative.
24	DoD		T	4.1.4.1.c	The document references "active duty." Does active refer to uniformed service or only DoD military service? Contractor, civilian, and active duty is not an exhaustive list.	Need to clarify the intent of the active duty line and make the list exhaustive.
25	DoD		T		The required operation for RSA is to decrypt and for Elliptic Curve to sign, but in previous instances, the standard states that RSA or Elliptic Curve keys can be used. to sign for authentication, which is a base requirement. This requires RSA keys to encrypt.	Clarify the functionalities of the different keys. Clarify if both keys are needed to decrypt and sign. Recommend changing to RSA encrypt.
26	DoD		T		Trust Anchor Certificate Retrieval or Validation is not mentioned in the standard.	Recommend possibly adding Trust Anchor Certificate Retrieval or Validation.
27	DoD		T		Standard does not specify a specific public key authentication protocol.	Lack of specificity on the authentication protocol will not ensure interoperability. The biggest threat to our physical facilities is access provided via a flash pass. If an employee does not have to e-authenticate because the protocol is not supported at the local site, then the token is nothing more than a flash pass.
28	DoD		T		It isn't clear why symmetric keys are needed. It would weaken security if all cards are issued with same symmetric keys.	Recommend addressing this bullet.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
29	DoD		T		It is not clear whether high assurance cards are backward compatible with low assurance access points, and therefore, have the capability to present stored value or signed value of the CHUID in addition to the cryptographic response to a challenge required by the high assurance card.	
30	DoD		T		Definition of the relationship between the contact and contactless chips on the card is needed.	Explain how both chips will be tracked in the PIV card management system. For example, is it possible to lose physical access rights, but still retain your card for logical access or vice versa?
31	DoD		T		The existence of a copy of a signed object on a card does not mean that the card is not a forgery. The contactless interface will provide the signed object to any reader. It is only marginally harder to copy the signed object to a card than it is to create an unsigned object.	Clarify that possession of a signed object does not guarantee that the card is not a forgery. The signed object only guarantees that the forger had some level of access to the original card at some point.
32	DoD		T		Since this is a cryptographic module, why isn't the PIN requirement the FIPS 140 requirement? As written, this will require two different PIN implementations.	Change to conform to the FIPS 140 activation requirement.
33	DoD		T		Ambiguous reference to key generation implies it could be done either on the card or off the card.	No mechanism is described for key escrow of a private key. Also, if the key pair is generated in an hardware security module (HSM), how is the private key loaded securely onto the card?
34	DoD		T		Life span of a key that is generated off the card should be included in the standard.	If keys are generated in the HSM and then stored on the card, a mechanism must be in place to deactivate the key in the HSM when the certificate (associated to this key) expires or is revoked.
35	DoD		T		Is there a requirement for a separate PIV authentication key, or can the same key be used for PIV authentication and other digital signature functions?	Clarify if the different keys mentioned can meet multiple key requirements.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
36	DoD		T		Since the keys are optional, except the PIV authentication key, what is the impact if they don't conform to the requirements?	Clarify the impact of key size on implementing optional keys. If not, DoD will be out of compliance. The year 2007 is not long enough to change out the card and issuance inventory.
37	DoD		T		The x.509 certificate shall include the FASC-N in the subject alternative name extension to support physical access procedures.	DoD currently stores subscriber email address in this field
38	DoD		T		Testing and Certification: This specification must contain a certification process to make sure that the implementation of PC/SC is consistent and interoperable.	DoD uses an industry testing and certification process for PC/SC. Strongly recommend adding the following:
39	DoD		T		Additional Needs to ensure card and reader communicate:This specification lacks finite details required to ensure the cards and readers communicate.	If any of the below items are adjusted or are not synchronized, readers will not be able to communicate with cards. DoD strongly recommends adding the following mandatory elements to the reader specification:Protocol: T=1 and T=0; Frequency: 1-5 MHz; Data Exchange Rate: 9600bsp to 115,200 bps or greater;Voltage: 3V and 5V
40	DoD		T		National Information Assurance Partnership (NIAP) Common Criteria requirements are not addressed.	Need to address what requirements exist for NIAP common criteria.
					“assure the interoperability of products and services developed in accordance with the standard”	Develop specific interoperability guidelines and reference them in the standard as a requirement.
41	DoD		T		The DoD smart card is built on Java Card, with applets programmed to recognize GSC-IS commands. CAC applets would need to be recoded to recognize FIPS 201 commands. Recoding would also involve changes in logic and data structure. Recoded applets would need to be loaded onto every card in circulation; otherwise, three concurrent solutions would exist.	

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
42	DoD		T	A.1	The first paragraph of A.1 states that "all of the cryptographic modules in the PIV system (both on-card and issuer software) shall be certified to be FIPS 140-2 Level 2 (or higher) compliant." However, some cryptographic modules that are used by client software to establish Secure Socket Layer (SSL) are only Level 1 validated.	Recommend clarifying which specific modules must be level 2 validated rather than a general "all" statement.
43	DoD				It is not clear whether the table requires both or either algorithms. It will be hard to use both algorithms. Additionally, there is no transition plan.	
44	DoD		T	Section 5.2.3.1	It is unclear what value Subject Information Access (SIA) provides. If authority information access is used, there will be redundancy between SIA in a CA certificate and the AIA in a subordinate certificate	
45	DoD		T	Section 5.2.3.5	"The definitive OCSP responder for each certificate shall be specified in the AIA extension"	The AIA extension is optional. DoD is configuring the OCSP client plug-in with the ULR of the definitive OCSP responder.
46	DoD		T		Having each CA that the responder responds for requires many certificates in a large PKI such as the DoD.	Have a single CA sign a responder's certificate. This works for many of the responders in the marketplace, but is not strictly in conformance with the OCSP spec.
47	DoD		T	Section 5.2.3.6	The requirement to assert the Common Policy OID in certificates after 2007 means those agencies will have to fully comply with the Common Policy. However, DoD and other agencies (not legacy) with their own PKIs fully meet the requirements of the Federal Bridge Certificate Authority (FBCA) Medium Assurance, but do not necessarily track with the requirements of the Common Policy. FICC requirements that Agencies either cross-certify with the FBCA or use a SSP that meets the Common Policy should be reflected in the document.	

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
48	DoD		T	Section 5.3	The DoD has addressed the issue of support contractors through the External Certification Authority (ECA) PKI. The ECA CP has been approved at Medium Assurance to join the Federal Bridge. This PKI should be considered as a complement to the SSP model, which is designed for Federal employees.	
49	DoD		T	Section 2.2	Registration authority can not perform background checks. Someone else will have to verify that it was done. Does this mean a person awaiting an investigation can't get an ID card?	Should not be the registration official who conducts the background investigation. If required, it should be verified to him/her. What happens to people who have a delay in
50	DoD		E	Table 4-7	The spec references a 30:1 ratio using JPEG. I believe author meant to say 30:1 using JPEG 2000.	Would recommend specification using JPEG 2000 for compressing rather than the old JPEG compression.
51	DoD		T	p26, Section 4.2.2 p43, Section 5.2.3 p46, Section 5.2.3.6	In sections 4.2.2, 5,2,3. and 5.2.3.6, FIPS 201 requires that all certificates assert the Common Policy OID. However, the FICC has stated that agencies must either have their existing agency PKI cross-certified with the	Align FIPS 201 requirements with FICC requirements that certificates must either assert the Common Policy OID or be issued from an agency PKI that has been cross-
52	DoD		T	p45, Section 5.2.3.3	In addition to stating the requirement to assert the Common Policy OIDs, FIPS 201 section 5.2.3.3 restates the Common Policy requirement for CRL publication every 18 hours. The DoD PKI currently issues CRLs every 24 hours. Because of the scale of the DoD PKI, issuing CRLs requires a significant amount of processing time for the DoD CAs. Also, the large size of the DoD PKI CRLs (over 40mb total size) means that increasing the frequency of CRL publication and distribution will have a significant impact on bandwidth and the usability of PKI within the DoD.	Either require CRL issuance frequency every 24 hours or delete this requirement from FIPS 201 since it is addressed in both the FBCA CP and the Common Policy.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
53	DoD		G	p43-46, Section 5.2.3	The number of distinct documents, each with their own set of requirements that do not correlate, is growing (e.g., FBCA CP, Common Policy CP, FIPS 201, Federal PKI Certificate Profiles, eAuthentication policy, SP 800-63, SP 800-73). As a result, attempting to determine specific requirements for a given implementation is becoming more and more difficult.	Rather than proliferating documents that do not quite map to each other, time should be taken to update a small set of standards / policies / etc. that clearly interrelate.
54	DoD		G	p40, Section 5.1.2 p45, Section 5.2.3.5	The document appears to require agencies to maintain OCSP responders, but does not fully address the implications of this requirement. Generally OCSP	Clarify the requirement for support for OCSP between agencies.
55	DoD		T	p28, Section 4.3	The table requires 2048-bit keys after 12/31/2008. This means that certificates issued with a three-year life span would have to be 2048 by 12/31/2005. Not all COTS PK-Enabled products support 2048-bit keys at this time, so the requirement for using them will likely cause application compatibility issues.	Extend the deadline for migrating to 2048-bit keys in client certificates to account for testing and COTS software capabilities.
56	DoD		T	p25, Section 4.2 p29, Section 4.3	If the FASC-N is required to be contained in the certificate, then the certificate issuance process must somehow be able to get this information and include it in the certificate request. Including the FASC-N in the subject alternative name extension is different than what the DoD PKI does today. For identity certificates, no information is contained here, for signature certificates, the email address and the Microsoft login UPN are contained here. The FASC-N extension is not part of the X.509 standard and should be considered a custom value. What is the OID for the FASC-N?	Recommend deleting the requirement to include the FASC-N in the certificate. If not, provide additional information for the inclusion of the FASC-N in the extension and allow time to integrate this capability.
57	DoD		T	p17, Section 4.1 p24, Section 4.1.6	This document limits FIPS 140 applicability to the card and to PIN-based cardholder activation. However, FIPS	Add the FIPS 140 requirements for biometric-based cardholder activation.
				General	HSPD-12 states, "...the heads of executive departments and agencies shall...require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems."	Provide guidance on the community that HSPD-12 and FIPS 201 apply to.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
58	DoD		G	(specific references include p v Item 6, p v Item 8, p1 Section 1, and p4 Section 2.1)	This statement is unclear as to whether it applies to only those people who would normally be issued an ID card for physical access to Federal buildings or all contractors that access Federal information systems. HSPD-12 also states, "the standard [FIPS 201] will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application." Although FIPS 201 contains background check requirements for four graduated position sensitivity levels, it does not contain any other references to graduated criteria. If logical access to all federal information systems is within scope of HSPD-12, FIPS 201 needs to address a lower level credential (such as a software certificate or a username/password) that does not require the issuance of a card for logical access.	Since the eAuthentication policy addresses four credential levels along with criteria for determining the minimum credential level for a given information system, recommend referencing this policy and the associated SP 800-53 for these types of credentials.
59	DoD		G	p3-7, Part 1 General comment	The process outlined in Part 1: (PIV-I) does not appear to be well thought out. General concerns with the process include: · It is manual, repetitive, people intensive, and time consuming, which will result in greater expense to the government. · It may not conform to current legal and procedural requirements. · While the process requires significant fact checking for the applicant, it does not describe verifiable authorization checking for communication between officials. · It appears to create a significant storage and archival requirement for privacy act sensitive data.	Coordinate with agencies currently performing identity proofing and background checks for new employees and contractors to update the process. Also, recommend using PKI capabilities instead of paper signatures to increase the overall assurance of the process and decrease time to complete.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
					· The process for issuing the physical credential is not strongly tied to the process of issuing the PKI certificate credential, which results in additional resources to verify the applicant identity prior to issuing the certificate. Specific comments for each of these concerns follow.	
60	DoD		G	p3-7, Part 1 General comment	The process outlined in Part 1: (PIV-I) is manual, repetitive, people intensive, and time consuming, which will result in greater expense to the government. There are five distinct roles defined, the applicant, the Requesting Official, the Authorizing Official, the Registration Authority, and the Issuing Authority. No individual is permitted to assume more than one of these roles. However, no justification is provided for why each of these tasks must be performed by a separate individual, and no guidance is provided as to whether there are any requirements for these positions to be occupied by Federal government employees. Applicants are required to present their identity source documents three times, once to the Requesting Official, once to the Registration Authority, and a third time to the Issuing Authority. Each of these people must obtain the photocopies from the earlier official as a part of the process. If these photocopies become decoupled from the application, must the applicant start over? Adding additional paperwork does not seem to be improving the way the Government operates. Also, what if the applicant brings different identity source documents?	Recommend stating the requirements of what actions must be performed and allowing agencies to determine the best process for meeting these requirements instead of specifically defining a process that will not work in all environments. Also recommend the use of electronic media such as databases and digital signatures to facilitate information collection, dissemination, and verification.

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
					For members of the National Guard, individuals are physically available only one weekend a month at geographically distinct stations. If each of these stations is required to have four distinct roles represented by four distinct individuals, and processing can only occur when guard members are present, completing the process for issuing a permanent ID card could take up to three months. However, the permanent ID card is needed to perform guard duties.	
61	DoD		G	p3-7, Part 1 General comment	The process outlined in Part 1: (PIV-I) may not conform to current legal and procedural requirements.	Coordinate identity proofing processes with the owners of existing requirements, such as INS for I-9 OPM for background checks, and State Department for host nationals. If current forms cannot accommodate guidance as specified, either negotiate changes to the forms themselves or use different forms.
				Section 5.2.1.1)	The process states that at least one of the documents presented for employment verification shall be a valid State or Federal Government-issued picture ID. However, not all of the documents listed in I9 List A or combination listed in I9 List B and C are State or Federal Government-issued picture IDs, and I9 states that "Employers CANNOT specify which document(s) they will accept from an employee."	Cross-check FIPS 201 requirements with existing laws such as GPEA, Privacy Act, and E-SIGN.
				p14, Section 3.3.2	The standard creates additional paper based processes that doe not appear to be in line with the Government Paperwork Elimination Act.	

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
					The standard may not meet privacy act requirements. There is a lot of personal data collected, transmitted, and stored. Justifications for why this information, such as marital status, is needed are not provided, nor are protections for transmission and accessing stored data described. Collection and transmission of fingerprint information may also be an issue, especially for employees or contractors at US facilities outside the US who are not US citizens.	
62	DoD		G	p3-7, Part 1 General comment	The process outlined in Part 1: (PIV-I) does not describe verifiable authorization checking for communication between officials. Officials are expected to rely on paper ink signatures from other officials, but don't have any way to verify that the signer is the named official or that the named official is authorized to act in that capacity. This lack of validation of officials decreases the overall assurance of the process. Will the authorizing official be required to validate that the requesting official is authorized to make the request? How will this be done? If the authorizing official is not required to validate the authority of the requesting official, then what added security does having a requesting official add to the process? Why are the registration authority and issuing authority required to be separate people? Again, does the issuing authority have to validate the credential of the requesting authority? What added security does separating these two roles bring?	Recommend requiring PKI based digital signatures that can be validated against a list of authorized individuals. Also, decreasing the number of individuals in the process will streamline the process and decrease the requirement for validating the authorizations.

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
63	DoD		G	p3-7, Part 1 General comment	The process outlined in Part 1: (PIV-I) appears to create a significant storage and archival requirement for privacy act sensitive data. All of applicant registration data collected at the onset of the registration process is stored in the Registration Repository. Is there a minimum of information that must be included in the repository? Is additional information from the PIV request required to be captured such as names of authorities involved in the process? How long must information be stored?	Provide clarification on the requirement to store and archive data elements related to the identity proofing process.
64	DoD		G	p3-7, Part 1 General comment	The process outlined in Part 1: (PIV-I) for issuing the physical credential is not strongly tied to the process of issuing the PKI certificate credential, which results in additional resources to verify the applicant identity prior to issuing the certificate.	Integrate the digital certificate issuance process with the card issuance process.
65	DoD		T	General	The standard does not define the use of any unique identifier that remains with the individual throughout the life of that individual's association with the agency. PKI certificates and cards expire, so keys associated with certificates and the FASC-N have limited life span. In order to tie an individual with appropriate attribute and authorization information stored in directories or other locations, and to be able to synchronize information across directories, an identifier is required. The DoD uses the EDIPI for this purpose.	Include a unique identifier that does not change over the life of the individual's association with the agency.
66	DoD		T	p29, Section 4.3	The user is not required to enter the PIN for each action for the authentication or key management keys, but is required to do so for the signature key. However, current smart card technology does not support the capability to require the PIN to activate one private key on the card but allow caching for activation of a different private key on the same card. For example, the DoD CAC PKI applet either requires the PIN for every action or allows a timeout for all actions.	Allow PIN caching for all transactions until technology supports setting distinct rules for different private keys within the same key store on a smart card.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
				P43, Section 5.2.3.2	Also, Section 5.2.3.2 requires card activation each time a key management key is used even though Section 4.3 allows PIN caching for key management keys.	
67	DoD		G	p6, Section 2.2.1	It is unclear how all agencies will be able to verify validity with the document issuer for all types of documents.	State acceptable mechanisms for verifying the validity of documents, such as using a commercial identity verification service to verify the identity of documents.
68	DoD		T	p23, Section 4.1.5	Section 4.1.5.2 calls for the CHUID to be stored as a transparent file in the root file system of the Card Manager to facilitate rapid retrieval for physical access control applications. The DoD PKI presently uses a unique ID, the EDIPI and not the CHUID.	Recommend that OMB consider this in their plans to issue guidance regarding agency development of transition plans to part 2.
69	DoD		T	p27, Section 4.3	The “authentication key” mentioned is also a signature key, as PKI-based authentication is performed through a digital signature operation. The document is unclear whether the signature key must be separate from the authentication key or if the two could be combined.	Clarify whether the signature key must be separate from the authentication key or if the two could be combined.
70	DoD		T	p30, Section 4.4	Current estimates for card storage is 36k bytes – 12k for card management, 22k for two signed fingerprint images, and 2k for PKI certificates. PKI certificates average 2-3k per certificate, so 9k may be required for storage of the authentication, signature, and key management certificates. If facial images are to be stored in addition, the total card storage requirement is significantly greater than the storage available on the card, and will have a significant impact on per-card costs.	Re-look at the requirements for storage on-card to determine if they can be offset by using PKI-based authentication to access information in centralized databases.
71	DoD		T	p43, Section 5.2.2	Section 5.2.2 describes an alternate process for an applicant to generate cryptographic key pairs and obtain corresponding certificates at a later time other than when they are issued their PIV card. If the applicant completes the issuance process from their own workstation. It is unclear what is used to ensure that the required keys are actually generated on the token and not in RAM on the subscriber workstation.	Please clarify what is used to ensure that the required keys are actually generated on the token and not in RAM on the subscriber workstation in the event that the applicant generates their own key pairs on their own workstation.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
72	DoD		T	p46, Section 5.2.4.2	Section 5.2.4.2 states "PIN resets may be performed by well laid out and documented procedures by each individual agency." PIN reset can be a significant security hole if not protected adequately. However, this statement places no requirements on the security goodness of PIN reset.	Add the following sentence: Documented procedures shall specify security measures that will be taken to ensure PIN reset is being requested by the PIV cardholder.
73	DoD		G	p5, Section 2.2	The terminology used in this section is non-standard. Generally, a registration authority (RA) is a standard certificate management authority role in PKI who issues PKI credentials, not the person that performs background checks.	Do not use terms of reference in the PIV model that conflict with already established, commonly acceptable terms and definitions of those terms. This will lead to confusion. Use another term not already commonly acceptable such as Registration Official.
74	DoD		E	p15, Section 3.3.3 (and Annex E)	Section 3.3.3 refers to I&A (Identification and Authentication) using the standard definition of these terms. However, the glossary defines authentication as the process of establishing confidence in user identities. Inconsistent terminology.	Update glossary definitions to align with National Information Assurance (IA) Glossary definitions
75	DoD		E	p17, Section 4.1.3 (and other sections)	The first four outline levels are numbered, but then the outlining switches to letters. Inconsistent formatting	Maintain consistent headers using number format (e.g., 4.1.1.1, 4.1.1.2 instead of 4.1.1.a, 4.1.1.b).
76	DoD		E	p40, Section 5.2.1	Section 5.2.1 is a duplication of Section 2.2. Confusing document layout.	Refer to the earlier section instead of including the text twice.
77	DoD		E	P13, Section 3.3 p43, Section 5.2.3	The term Key Management is used to refer to key pairs associated with certificates that can be used for	Refer to the components of the PKI as "PKI Components" and to encryption keys as "Key
78	DoD		T	p47, Section 5.2.4.2	Section 5.2.4.2 states "Agencies are required to have procedures in place to update all servers in one hour in the case of such an emergency." For agencies with a globally distributed population and servers such as the DoD, this requirement will be costly to meet.	Re-look at the requirement to either better define what is meant by "all servers" or use a more realistic time frame.
79	DoD		E	p47, Section 5.2.4.2	Given the political sensitivity of the "terrorist watch list," recommend using a different example.	Omit the example or use a different one.
				p51, Section 6.1.2	Digital signature checking and expiration date checking are listed as optional. Checking the digital signature on	Recommend requiring check of the expiration date.

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
80	DoD		T		the CHUID is one of the mechanisms that prevents forgery, and the expiration date is also an added protection. Why are these listed as optional?	Since validating the digital signature of the CHUID adds complexity to the card authentication, and may not be available in all environments, state that the digital signature verification is "recommended" instead of "optional."
81	DoD		T	p53, Section 6.1.5	The first item in the authentication mechanism states "The reader issues a challenge string to the card and requests an asymmetric operation in response." Technically, the challenge string is not issued to the card, the challenge string is issued to the workstation, which computes the hash, and the hash is provided to the card for encryption.	Update the text for correctness.
82	DoD		T	PIV II, Sec 4.1.5.1 and 4.1.6.1	The performance of the on-card biometric matching is questionable, especially if the standard calls for the use of images rather than templates. Storage space on the chip will be an issue if the images are stored on the card along with an on-card matching capability.	Recommend referencing the tempate standard (pending availablity) when discussing the on-card matching functionality.
83	DoD		T	4.1.5.2	Storing biometric images as transparent files in the root file system of the card manager **is a** high-security risk. Because individuals have a limited number of biometric features, security mechanisms to protect the biometrics should be a high priority, especially if a biometric image will be stored in the transparent file.	Because rapid retrieval is a requirement in physical access control applications, recommend the use of the fingerprint minutiae template standard. The template is much smaller than the image and therefore will faciliate a faster transaction between the card and the application system.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
84	DoD		G	4.4.2	The proposed standard requires two fingerprint images and one digital photo on the chip for facial recognition. This will consume more than 50% of the space available on the 64K card. Storing template minutiae rather than biometric images significantly reduces space requirements. Unanswered questions remain regarding the security of using IMAGES rather than template minutiae. The use of images is of particular concern from a privacy aspect and also because each person has a finite number of biometrics available, should one be compromised.	Recommend changing the biometric requirements on the card from images to template minutiae. This should be implemented when (1) interoperability specifications for biometric template minutiae matures and compliant products are available from multiple vendors, and (2) card capacity increases to adaquately accommodate the size requirment. Additionally, security measures needed to protect biometrics from compromise should be assessed and prescribed in the standard.
85	DoD		G	"	Because the draft standard mentions the MINEX 04, it needs to address the adoption of the minutiae template standard after successful testing and evaluation.	Recommend that the fingerprint minutiae template standard be adopted as the standard for fingerprints based on successful MINEX 04.This standard will also allow the use of biometrics with the contactless portion of the PIV card.
86	DoD		G	6.2	Authentication for physical access control does not address the use of biometrics especially in the contactless portion of the card.	Recommend that the standard address the use of biometrics in the contactless portion of the card. Since storing images on the contactless portion of the card will also be an issue, recommend the use of fingerprint minutiae template standard.
87	DoD		G	Annex E	Verification (1:1) and identification (1:N) biometric functions are very distinct and serve very different purposes.	Recommend futher explanation of the verification (1:1) and identification (1:N) functions.
88	DoD		T	4.4.5.5 Face Compression	The spec references a 30:1 ratio using JPEG. I believe author meant to say 30:1 using JPEG 2000.	Would recommend specification using JPEG 2000 for compressing rather than the old JPEG compression.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
89	DoD		T	5.2.4.1 Renewal	The specification does not mention how or why the fingerprint could be used from the old card.	Recommend clarification as to why the fingerprints from the old card would be moved to the new card. The biometric information in the central repository would be used to verify that the individual in front of you is who he or she says they are and reload the fingerprint data from the repository.