Submitted by: Tin T. Cao, Dept. of State - IRM/OPS/ITI/SI/IIB
Date: 1/19/2005

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
FIPS 201						
1	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E	ExecSum, pg iv, paragraph 2 (Category of Standard)	The Category of Standard --Information Security-- is a misnomer. This standard deals as much with physical security and access control as it does with Information Security.	Revise to read, "*Category of Standard: Security Identification and Authentication / Access Control*"
2	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E	ExecSum, pg iv, paragraph 3 (Explanation)	Most Federal agencies and many Federal contractors are familiar with the Federal Identity Credential (FIC) that is/was building on the Federal Public Key Infrastructure (itself pre-dating but serving to implement GPEA, E-Sign, and E-Gov legislation).	Recommend that FIPS 201 at least make mention of these previous efforts to clarify that the PIV is (a) an outgrowth of them; (b) a replacement of them; and/or (c) an additional, but similar, requirement. If for no other reason, this will allow agency senior management to understand its derivation and to use that logic in support of business case and budget development.
3	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E	ExecSum, pg v, paragraph 8 (Implementations-third subparagraph)	The second sentence is confusing; "agencies accredit issuers who issue…to employees and contractors…" If the PIV is for Federal **employees and contractors** then are agencies accrediting themselves, some other entity, or are they being accredited themselves by an unnamed central accreditation authority?	Revise to read, "…agencies*, or other accredited issuers,* issue identity credentials for Federal employees and contractors until…"
4	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	ExecSum, pgs v-vi, paragraph 9 (Effective Date)	This section continues the split between PIV-1 and PIV-2, but introduces a degree of uncertainty. Agencies must meet the PIV-1 standard by October 2005, but the deadline for meeting the more important, costly, and time consuming effort of PIV-2 is not specified. As a result, agencies cannot even begin the budgeting process for FY 2007.	Recommend that, at least, the date for the OMB announcement be included, if not the actual implementation deadline.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, 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
5	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E	ExecSum, pg vi, paragraph 10 (Qualifications-first subparagraph)	The phraseology, “Organizations adopting this standard …” implies that adoption of this standard contains a certain degree of voluntariness, which it does not, and which appears inconsistent with paragraphs 6 and 11.	Revise to read: “*Upon adopting this standard,* organizations must be aware …”
6	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	ExecSum, pg vi, paragraph 10 (Qualifications-fourth subparagraph)	This section correctly points out the need for flexibility, but then calls for a review at a five year interval. With the pace of science and technology, this if far too long for mandatory review of this standard.	Revise to read, "…agency will review this standard every *two* years to assess its adequacy."
7	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E	ExecSum, pg vi, paragraph 11 (Waivers)	The qualification contained in the second sentence of the preliminary draft recognized the realities of adopting this new standard. Given the lack of available funding, simply saying that the standard is not waiverable is unrealistic.	Restore the second sentence, or a comparable caveat, from the preliminary draft.
8	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Introduction, Section 1.3 (Document Organization), pg 2 (second subparagraph)	The third sentence introduces certain confusion, by stating that, "This standard does not restrict the agencies from adopting additional alternatives." Yet the fifth sentence mandates that portions be "...followed literally and explicitly…"	Clarify the intent of the third sentence. Revise to read, "*Within the bounds established by this standard, agencies are not restricted from adopting additional alternatives.*"

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
9	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E/T	Part 1, Section 2.2 (Identity Proofing and Registration Process), pg 4 (first subparagraph)	Although the provision that one individual may not assume more than one role in the process has a certain merit, it ignores a basic reality, i.e., who issues, registers, authorizes, requests, and applies for the first card within an agency at any given location? Can one rely on an individual whose own identity has not been proven and verified by receipt of a PIV credential? Further, some agencies--particularly those in remote and/or overseas locations--have offices and posts with fewer than five cleared American employees, some of which are senior employees (e.g., GS-15, FS-01, SES/SFS) which automatically forces one or more of these individuals to assume multiple roles.	None; this is a conundrum that will force waivers until such time as the PIV infrastructure is established and functioning.
10	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 1, Section 2.2 (Identity Proofing and Registration Process), pgs 4-5 (second & third bullets)	This paragraph does not adequately address the responsibilities and legal authority of the Requesting Official and the Authorizing Official. While the authority of a supervisor may be unquestioned regarding Federal employees, requiring contractor personnel to divulge information protected under the Privacy Act without provision of a specified warning notice to persons not formally recognized as investigators may pose a legal challenge.	Clarify/expand the responsibilities and legal authority of all Officials and Authorities identified in this paragraph in succeeding paragraphs. Specify the requirement to adhere to the provisions of the Privacy Act and provide, at a minimum, guidance on the development of a suitable Privacy Act notice.

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
11	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), pg 5 (second subparagraph)	This paragraph establishes the requirement that an applicant apply for a PIV card as part of the vetting process for Federal employment. Aside from the fact that this totally ignores contractors, the vetting process will become even more resource intensive and time consuming, and card issuance will depend entirely on whether or not an actual hiring action occurs. Further, many of the requirements—identity verification, background checks, determination of Requesting (Sponsor?) Official and Authorizing Official—are already part of the hiring process. While the current system is imperfect, establishing a mirror image of what already exists (as this appears to do at this point) is wasteful, and runs counter to both HSPD-12 and several other Presidential and OMB mandates. Finally, until an individual is actually hired and the Requesting and Authorizing Officials are identified, the PIV vetting process is wasted effort. It is also unclear as to whether any of these authorities belong to the agency hiring the individual or to a separate agency.	Recommend that this element be reconsidered to mandate that the background vetting requirements (e.g., identity verification, background check) become an integral part of the hiring process, and that standardized, and potentially shared, databases be established. Further, the actual application process should be made a mandatory part of the initial hiring procedure, such that between the time an individual is informed and appears on the first day to in-process at a specific organization, the PIV can be final vetted, approved, and produced. Additionally, recommend that clarifying language be included to identify if these authorities are a part of the hiring agency; if they are dedicated to this process full time, and if so, what types of offices such as HR, security are involved; and what special qualifications and training are required. Finally, recommend that contractor companies be required to submit the necessary background information as part of the VAR procedure, and/or be “certified” as the Requesting Official through the appropriate agency COR.
12	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), pg 5 (second subparagraph)	This paragraph (paragraph 2.2.4 notwithstanding) specifies that identity documentation come from the Form I-9 list, and that at least one be a valid state or Federal (presumably U.S.) Government ID. This is unnecessarily restrictive and unacceptable to the State Department, with nearly half of its "employee" work force comprised of foreign nationals employed in their native countries but all of whom must receive a State Department ID granting both physical and logical access.	Revise to read, "…Eligibility Verification *or equivalent national standard from the country of citizenship.* At least, one of the documents…*or national equivalent.*"

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	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), pg 5 (second subparagraph)	The process makes no provision or authorization for the use of electronic forms, in direct violation of the GPEA, E-Sign, and E-Gov legislation. Source documents can be scanned rather than photocopied, and an electronic form that accepts the digital signatures of the necessary officials will eliminate a bureaucratic administrative burden on agencies. Further, the applicant may have some type of (personal) digital signature, which is valid under E-Sign legislation.	Revise to read, "…Government-issued picture ID. The PIV Requesting Official shall *prepare and* submit the PIV request and *either scanned or photocopied* copies of identity source documents for the Applicant *in electronic form* to…"
14	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), pg 5 (final bullet)	The requirement for signatures is non-specific, but would usually be taken to mean "wet ink." Again, this ignores the requirements of GPEA, E-Sign, and E-Gov.	Revise to read, Signatures *(digital or ink*) of the…"
15	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), Tables 2-1 & 2-2, pg 6	Position sensitive levels have existed within the Federal Government for many years (i.e., Critical-Sensitive, Critical-Nonsensitive, Sensitive, Nonsensitive) and are well documented and understood by those offices and personnel most likely to have to implement the PIV. Titles, such as Low, High, etc., are vague and open to interpretation, and should be left to the intellectually challenged.	Change the titles of Low, Moderate, etc., to titles that are already documented, understood, and in common use throughout the Federal government.

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
16	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), pg 6 (first subparagraph)	The assignment of responsibilities in this paragraph is ill-considered and does not reflect existing or potential capabilities. First, the Registration Authority (RA) is not an individual but an office, in most cases. Therefore, there is a potential loss of accuracy, reliability, and accountability. Second, requiring the RA to collect fingerprints—unless a biometric tool is used—also requires specific training and acceptance of the presumption that all RAs are capable of performing this task adequately. Third, unless and until this document specifies that all Federal activities hold the responsibility and authority for performing background checks, RA offices and personnel will lack the specialized training to perform more than a cursory records check (i.e., of lower quality than a NAC/NACI).	Recommend that this entire portion be reviewed with inputs from multiple Federal activities currently chartered to conduct background investigations.
17	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), pg 6 (first subparagraph)	Visual inspection of identification documentation is, at best, a cursory proof of validity. This presumes that forged, stolen, modified identity source documents can be identified by visual inspection alone. Unless and until the identity source documents (e.g., I-9 documents) are sufficiently standardized and secured, visual inspection is futile. Further, it requires that the Registration Authority be knowledgeable and trained in this technique, and able to recognize a wide variety of identification. Finally, it assumes that the document was issued by a U.S. legal entity (e.g., Federal, state, local government or tribal council), is printed in English, and so forth.	Consider some form of verification other than visual inspection of the source identity documentation.

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
18	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), Table 2-2, pg 6	The requirement for verifying the validity of an Applicant's identity source documents is impractical. This requirement forces the PIV Registration Authorities to contact states, local jurisdictions, tribal councils, and other Federal agencies (depending on the documentation presented). However, it does not provide for those entities to respond or to respond in a "timely" manner. The requirement creates an unfunded mandate for those activities to receive, process, and respond to literally millions of requests initially, and tens of thousands more on an annual basis.	None; this is a conundrum that will force waivers until such time as the PIV infrastructure is established and functioning; and potentially on a permanent basis. There is no benefit to state and local jurisdications, nor is there any mechanism to coerce compliance.
19	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 1, Section 2.2.1 (Identity Proofing and Registration of New Employees and Contractors), pg 7	This requirement establishes a significant records keeping burden on Registration Authorities, particularly if these records are maintained in hard copy. There does not appear to be stated criteria for retention by the Registration Authority or the need to archive these records on a more permanent basis. Further, this creates a new/duplicate "system of records" as defined by the Privacy Act, but the requirements of that law do not appear to have been considered. Finally, if the PIV process is divorced from the hiring and clearance processes, it will result in an additional burden to both Federal and state/local governments to request, process, and store this information. State/local governments are very likely to request (additional?) payment for rendering these services that add to their already strained infrastructures	Revise to read, "…The Registration Authority shall be responsible to maintain*, in either paper or electronic form, and in accordance with the provisions of the Privacy Act*:" Further, recommend that this entire portion be reviewed with inputs from multiple Federal activities currently chartered to conduct background investigations

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
20	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 1, Section 2.3 (Identity Credential Issuance), pg 7	As noted in previous comments, this requirement makes no provision for the collection and retention of these records in electronic format--placing a significant records retention requirement on the Issuing Authorities.	Make some provision for the retention of this information in electronic format.
21	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 3.2.1 ((Agency Responsibilities), pg 11 (final bullet)	The wording of this bullet implies that a valid PIV will become the single mechanism to control and grant access to facilities and information systems (other disclaimers notwithstanding). The PIV establishes a mechanism to verify identity, but it does not address authorization or the mechanics of granting authorization. For example, an individual from one agency will not be able to enter another agency and logon to an IT workstation, regardless of their PIV level, unless they have a pre-established system account.	Revise to read, "…the PIV system to *facilitate the granting and control of access* to all people authorized…or information system *and pre-approved for such access in accordance with the visited agency's procedures.*"
22	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 3.2.3 (Oversight Responsibilities), pg 12 (final bullet)	OPM can be a responsible agency only for Federal civil service and military employees. There are potentially other categories of Federal employees not covered by OPM. Further, OPM has nothing to do with contractors, which are directly responsible only to the employing agency.	Add clarifying language to OPM's statement of responsibilities; and, add an oversight requirement for contractor employees (e.g., Defense Security Service, individual agencies, etc.)
23	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 3.3 (Functional Components), pg 12 (first bullet)	As specified in the Glossary, a "PIN" is typically comprised only of numeric digits. While in common use for physical access control, the established industry standard for logical access control (with or without a biometric) is the alphanumeric **password**.	Modify this bullet to allow the use of alphanumeric passwords for logical access control. Recommend that the continued reference throughout the document to the use of a "PIN" be changed to "*...an appropriate, personally held identifier (PIN, password, biometric, etc.)*."

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
24	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Figure 3-1, pg 13	As noted previously, the PIV Front End subsystem is keyed primarily toward physical access control (e.g., there is no "PIN Pad Device" attached to a computer system other than the keyboard, AND computers generally use an alphanumeric password rather than a PIN--defined as typically a numeric digit string)	Re-think the definition and design of the PIV Front End to reflect separate "front ends" for physical and logical access control.
25	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 3.3.1 (PIV Front-End Sybsystem), pg 14 (first subparagraph)	This normative paragraph specifies that the PIV card will have "…one or more embedded integrated circuit chips…" yet other sections of the standard appear to specify multiple chip types. In accordance with this paragraph, an agency could adopt the use of a contact chip only solution and not violate either the letter or spirit of the standard.	Decide what the normative solution will be (e.g., one chip, two chips, contact, contactless, etc.) and track that requirement throughout the standard.
26	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 3.3.1 (PIV Front-End Sybsystem), pg 14 (third & fifth subparagraphs)	As previously noted, PINs are not normally used for logical access control. Unless the intent is to force all Federal agencies to the use of a PIN (vice the established, industry-standard password), then every instance in which PIN is mentioned must be changed.	GLOBAL COMMENT: Revise every instance in which the term PIN appears be changed to "...*an appropriate, personally held identifier (PIN, password, biometric, etc.)*."
27	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 3.3.1 (PIV Front-End Sybsystem), pg 14 (fourth & fifth subparagraphs)	The discussion of biometrics throughout the document mixes (and confuses) implementation techniques suitable for physical access control with those for logical access control.	Beginning with this paragraph, clearly separate the uses and implementation techniques for physical and logical access control.

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
28	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 3.3.2 (PIV Card Issuance and Management Subsystem), pg 14 (second subparagraph)	As noted, the standard introduces confusion between implementation techniques suitable for physical access control with those suitable for logical access control. This paragraph specifies that biometric data will me stored in the Registration Repository, whereas Section 3.3.1/fourth subparagraph clearly states that it will be stored in card memory. The former, Registration Repository storage, is best suited to support physical access control where a certain degree of intra-/inter-agency comparison is desired; the latter, match-on-card, is best suited to logical access control where no inter-agency comparison is needed.	Revise to read, "All of the Applicant…stored in the Registration Repository *to support intra- and inter-agency comparison for physical access control. Biometric data to support logical access control is stored in the memory of the card.*"
29	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 3.3.3 (PIV Access Control Subsystem), pg 15 (third subparagraph)	This subparagraph clearly states that "…access control components typically interface…**optionally with the biometric reader**." Are agencies to presume that the adoption of biometrics (or at least biometric readers) is optional? Other portions of the document clearly specify that biometrics will be collected and stored in various locations.	Decide what the normative solution will be and track that requirement throughout the standard.
30	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1 (PIV Card Specifications), pg 17 (second subparagraph)	PKI policies specify that the card must meet FIPS 140-1/-2, level 2 requirements as a minimum for use as a PKI hardware token/cryptographic module used by Subscribers.	Include the appropriate reference to FIPS 140-1/-2, level X.

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
31	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.2 (Physical Security Tamper Proofing and Resistance), pg 17	While the need to develop standardized means of providing human-readable, tamper proofing and resistance is understood and applauded, the specification of a single method--despite allowing for "additional" rather than "alternative" methods--will force many/most/all of those agencies that adopted smart card-PKI-biometric technologies early to scrap their existing systems well before the anticipated life-cycle end dates; and, incur even greater, unprogrammed and unsupported costs re-issuing cards and PKI certificates.	Make the use of OVD and OVI one of a number of specified options, rather than the solution.
32	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 4.1.4.1 (Front of the Card (Mandatory)), pg 19	There are a number of deficiencies with the proposed topography, not the least of which is the mandated adoption of a format that while it meets the DoD business case, is not compatible with or acceptable to the business cases of other Federal agencies. Again, agencies that adopted smart card-PKI-biometric technologies early on are being penalized for their foresight and early adoption. This standard will cost these agencies (e.g., Department of State) several million in wasted funding and still more millions in halting on-going fielding, scraping existing systems, and re-issuing smart ID card/PKI hardware tokens and certificates.	Accommodate existing topologies until the projected life-cycle termination dates for those agencies that had previously adopted these technologies.
33	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.4.1 (Front of the Card (Mandatory)), pg 19	The mandatory specification “United States Government” and/or agency/department name, as well as the use of Agency Seal and other "mandatory" information, is dangerous and therefore unacceptable in an overseas environment where the individual is not within the protected confines of a military garrison or embassy compound.	Completely re-think the concept of a mandated topology to take into consideration the fact that for some Departments and Agencies these cards will be issued, used, lost, and/or stolen outside the U.S.

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
34	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.4.1 (Front of the Card (Mandatory)), pgs 19-20	The topography allows no modifications to suit agency-specific business cases (e.g., designation of persons authorized access outside of normal business hours, escort authority, specialized security clearances and access that might be readily apparent to visual inspection by either a guard or an employee within a specific high-security area).	Completely re-think the concept of a mandated topology to take into consideration the fact that, for some Departments and Agencies, these cards will be issued, used, lost, and/or stolen outside the U.S.
35	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.5.1 (Logical Credential Data Model), pg 23 (first bullet, first set)	The use of a PIN, while acceptable for most physical access control implementations, overlooks the fact that a PIN is generally considered to be below established industry standards for logical access control; and, violates most Federal logical access control regulations, which specify a 6-8 alpha-numeric password and frequently include requirements for upper/lower case and special characters among others. This “best business practice” has been ignored.	Recommend that this bullet either specify that the PIN be for physical access control and add an additional bullet to provide for the use of passwords in logical access control; or make provision for both in the same bullet.

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	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.5.1 (Logical Credential Data Model), pg 23 (fourth & fifth bullet, first set)	There is some question as to the value of mandating multiple biometric techniques for logical access control. While multiple biometrics are suited to physical access control, where inter-agency comparison is a requirement but involves a limited number of readers; their use in logical access control, where inter-agency comparison is unlikely due to the other requirements (e.g., a system account), would necessitate every agency provide multiple biometric readers at every workstation. Further, facial recognition technology requires the installation of photographic transmitters into areas processing both unclassified and classified information. Finally, by specifying both techniques as mandatory, the standard takes away from the agency a portion of their access control decision authority.	Revise the fourth bullet to read, "Two biometric fingerprints *and/or a biometric facial image, at the option of the agency.*" Delete the fifth bullet.
37	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.5.1 (Logical Credential Data Model), pg 23 (second subparagraph)	The last sentence of this subparagraph contradicts the mandate to include biometric data. Further, it implies that biometric technology is of limited use in CTC authentication vis-à-vis PINs, which are among the least secure of logical access control technologies. {For example, the State Department has implemented a biometric-PKI, match-on-card system for logical access control.}	Place biometrics and/or biometric-PKI, match-on-card solutions on an equal footing with PINs, passwords, and other CTC relevant techniques. (See also all previous comments regarding the use of PINs.)
38	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.5.2 (File Structure), pg 23 (third bullet, second set)	This bullet discusses the use of asymmetric or symmetric keys for supporting additional physical access applications in a section ostensibly devoted to logical access controls.	Revise to read, "…additional *logical* access…" -- OR -- delete this bullet.

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
39	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.5.2 (File Structure), pgs 23-24	There is some question as to whether CHUID, biometric, and other identity data stored as transparent files is actually secure and protected from disclosure, tampering, etc. Without some form of protection, (e.g., symmetric keys as specified in PACS, v2.2), all of this data is unprotected.	Specify a means (preferably symmetric keys) for securing the data stored in transparent files.
40	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.1.6.1 (Activation by Cardholder), pg 24 (second & third subparagraphs)	These two subparagraphs do not clearly differentiate between physical and logical card activation. As noted previously, PINs are normally acceptable for physical access control but lack the necessary rigor for logical access control even against the established industry standard password. Biometrics for physical access control, where intra-/inter-agency interoperability and comparison is vital, lose significant security and operational capabilities in a match-on-card implementation.	Recommend that this section be revised to differentiate between physical and logical access control implementations, as follows: [second subparagraph/first sentence] "For *physical access control* PIN-based cardholder activation… *For logical access control cardholder activation, the cardholder shall supply a minimum 6 character, alpha-numeric password.*" [third subparagraph/second sentence] "*For physical access control, the biometric information shall be transmitted and compared against an established database of pre-recorded templates and/or images. For logical access control, the* biometric information shall be transmitted... If the presented biometric..."
41	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.2 (Cardholder Unique Identifier (CHUID)), pg 25 (second subparagraph)	As noted previously, the standard specifies that agencies may adopt PIV cards with "one or more embedded integrated circuit chips." This paragraph specifies that the PIV CHUID be accessible from **both** contact and contactless interfaces.	Decide what the normative solution will be and track that requirement throughout the standard.

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	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.3 (Cryptographic Specifications), pg 27 (fourth subparagraph)	This paragraph introduces an agency-defined option into a section that is ostensibly normative: "That is, if an agency wishes to utilize an AES-based challenge response for physical access, the PIV card must contain storage for the AES key…" Therefore, if one agency chooses to adopt this technique, all agencies must accommodate the technique to achieve mandatory interoperability.	Decide what the normative solution will be and track that requirement throughout the standard.
43	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.3 (Cryptographic Speciications), pg 27 (fifth subparagraph)	The introduction of the expression, "…by a validated software cryptographic module." does not make sense. The PIV card itself is a hardware cryptographic module, therefore how and why is the use of a software module envisioned.	Decide what the normative solution will be and track that requirement throughout the standard.
44	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.3 (Cryptographic Specifications), pgs 27-28 (sixth subparagraph)	This paragraph does not make provision for a key pair used for data encryption (e.g., encryption of email, financial transactions, etc.)., which are an integral part of PKI operations. Is it the intent of this standard to prohibit such usage and/or require that agencies field another card to accommodate such use. Further, the derivation and use of the "key management key" and the "card management key" is not known or specified in this document.	Revise to read, "…and *five* types of optional keys:; then add the following bullet: *The encryption key is an asymmetric private key support document encryption and is optional;*"
45	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.3 (Cryptographic Specifications), pg 28 (first subparagraph)	As noted previously, PKI requires that hardware cryptographic tokens satisfy FIPS 140-2, Level 2 requirements. This requirement should also be included in paragraph 4.1 above. Further, this requirement increases the requirement from a Level 2 to a Level 3 smart card in the hands of the individual card holder. Even if no other card requirements changed, this will require that all agencies that have already fielded a smart card/PKI hardware token to replace all issued cards.	Review the requirement for a FIPS 140-2, Level 3 card in the hands of individual cardholders as potentially an unnecessary expense with little security gain.

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
46	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Table 4-5, pg 28	As noted above, the standard does not make provision for the use of PKI encryption capabilities. This is unacceptable to the Department of State.	Add Encryption Key with the same standards as digital signature
47	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.3, pgs 29	Again as noted, the standard does not make provision for the use of PKI encryption capabilities. This is unacceptable to the Department of State.	Add Encryption Key with the same standards as digital signature
48	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 4.4 (Biometric Specifications), pg 30 (third subparagraph)	If the recognition rates for facial images are so unsatisfactory and sensitive to external conditions, why specify this biometric for use by Federal employees and contractors. In addition, the facial image will require between 20-30 Kbyte of storage space, necessitating many/most/all agencies with existing smart card programs to upgrade to a larger storage card.	Review the requirement for the use of a facial image biometric.
49	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.4.1 (PIV Registration (Biometric Enrollment) and Issuance, pg 31	The use of the facial recognition technique for logical access control is ineffective and inappropriate. As stated in the standard, facial recognition is less effective than fingerprints, and requires fielding an additional desktop reader at every desktop in every agency. Further, the use of facial recognition places a photographic transmitted in office areas where processing of both unclassified and classified information occurs.	Limit the use of facial recognition technology to physical access control only, if used at all.

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
50	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.4.2 (Fingerprint Representation), pg 31 (first subparagraph)	While fingerprint images do offer the greatest degree of interoperability at this time, an image (a.k.a. a picture) provides the lowest level of security for this technique. The need for interoperability in logical access control implementations is nearly non-existent. Further, the size of the captured image is excessive given the limited storage space available on currently approved, commercially available smart card integrated circuit chips. Finally, as written, this section arbitrarily dismisses any use of other fingerprint implementations.	Specify that fingerprint images are suitable for physical access control implementations, but allow other fingerprint methods to be used in implementations in which the need for interoperability is limited or non-existent.
51	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 4.4.3 (Fingerprint Requirements for Biometric Enrollment), pg 31 (first subparagraph)	Collection of suitable/usable rolled fingerprints is an acquired skill, requiring a certain degree of training and practice. It is illogical to assume that Registration Authority personnel across all Federal agencies will have the necessary skills to immediately implement this aspect of the program.	Eliminate the collection of rolled fingerprint images.
52	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 4.4.3 (Fingerprint Requirements for Biometric Enrollment), pg 32 (final subparagraph)	Requiring agencies to commence mandatory collection of fingerprint data in March 2005 is unrealistic. The final standard will not be published until late February 2005, forcing agencies to acquire this capability, establish procedures, processes, storage databases and collection facilities, and train Registration Authority personnel within a matter of weeks. In accordance with HSPD-12, agencies are not even required to have program plans in place until four months after promulgations of the standard.	Postpone the requirement to submit fingerprints beginning in March 2005 until at least the required program activation 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	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.4.4 (Fingerprint Requirements for Identity Verification), pg 34 (first subparagraph)	While the fingerprint requirements for identity verification may be suitable for physical access control where interoperability and cross-agency verification are important, these requirements are unsuited for logical access control where interoperability is neither feasible nor required. Other fingerprint implementations are equally suitable and more secure than plain images for logical access; and the standard mandates that alternative methods of logical access control be available.	Specify that these requirements are for physical access control, but serve only as one potential alternative for logical access control.
54	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.4.5.8 (Quality), pg 37	Although the need for quality facial images is not disputed, the established requirements give the impression that agencies will have to establish rigidly controlled photographic capabilities. While this may be less burdensome in domestic facilities, it represents a major undertaking in remote and overseas locations.	Recommend that, as with fingerprints, the capture of acceptable facial imaging may be unobtainable in certain situations and/or with certain subjects
55	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T/E	Part 2, Section 4.4.6 (Protection of Biometrics), pg 38 (first subparagraph)	The terms CMS and CBEFF are not defined within the document. Further, if the use of symmetric and asymmetric (a.k.a. PKI) is mandated throughout the document, why is a separate technology introduced at this point.	Review the introduction of CMS external signatures for this one purpose, and if necessary, offer some explanation as to the value over symmetric and/or asymmetric digital signatures.
56	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 4.5.3 (PIN Pad Specifications), pg 39	As noted repeatedly throughout the comments to this document, the use of a PIN is suitable only for physical access control.	Eliminate the use of a PIN for logical access control; revise the third sentence as follows: Where the PIV card is used for logical access… the *use of a PIN shall be replaced with either a minimum 6 character, alpha-numeric password entered using the computer's keyboard, or by a biometric.*

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
57	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2,Section 5.1.2 (PKI Repository and OCSP Responder(s)), pg 40 (first & last subparagraphs)	This paragraph requires agencies to establish dual reporting channels for card and key status information. Many/most/all agencies with operational PKI do not maintain such a reporting capability now because it is not supported by the agency's business cases. This reporting should be alternative, rather than mandatorily dual capable.	Revise the first sentence to read: The PIV PKI Repository *and/or* On-line Certificate Status Protocol… Revise the last subparagraph to read: *Every CA that issues PIV authentication certificates may also operate an OCSP server…as an alternative.*
58	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2,Section 5.1.2 (PKI Repository and OCSP Responder(s)), pg 40 (third subparagraph)	There appears a presumption that all Federal agencies are (or will be) cross-certified -- in a two-way cross certification -- with the FBCA by the projected activation date; and that the FBCA will be capable of providing the envisioned level of support. Unfortunately, neither presumption is accurate. Only ≤ 25% of Federal agencies are currently cross-certified, and ≤ 25% more are actively pursuing cross certification. Further, attempts to use the FBCA for even the simple exchange of signed email has proven problematic due to directory issues.	None; this is a conundrum that will force waivers until such time as the FBCA--PIV infrastructure is established and functioning.

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
59	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E/T	Part 2, Section 5.2.1 (PIV Application and Approval), pgs 40-41 (first subparagraph)	As noted previously, this paragraph establishes the requirement that an applicant apply for a PIV card as part of the vetting process for Federal employment. The vetting process will become even more resource intensive and time consuming, and card issuance will depend entirely on whether or not an actual hiring action occurs. Further, many of the requirements—identity verification, background checks, determination of Requesting (Sponsor?) Official and Authorizing Official—are already part of the hiring process. This requirement also establishes a mirror image of what already exists, is wasteful, and runs counter to both HSPD-12 and several other Presidential and OMB mandates. Until an individual is actually hired and the Requesting and Authorizing Officials are identified, the PIV vetting process is wasted effort. It is also unclear as to whether any of these authorities belong to the agency hiring the individual or to a separate agency. Finally the process outlined here totally ignores the different procedures in and between agencies for contractors.	Recommend that this requirement be reconsidered to mandate that the background vetting requirements (e.g., identity verification, background check) become an integral part of the hiring process, and that standardized, and potentially shared, databases be established. Further, the actual application process should be made a mandatory part of the initial hiring procedure, such that between the time an individual is informed and appears on the first day to in-process at a specific organization, the PIV can be final vetted, approved, and produced. Finally, recommend that contractor companies be required to submit the necessary background information as part of the VAR procedure, and/or be "certified" as the Requesting Official through the appropriate agency COR.
60	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E/T	Part 2, Section 5.2.1 (PIV Application and Approval), pgs 40-41 (first subparagraph)	This paragraph specifies that identity documentation come from the Form I-9 list, and that at least one be a valid state or Federal Government ID. This is unnecessarily restrictive and unacceptable to the State Department, with nearly half of its "employee" work force comprised of foreign nationals employed in their native countries but all of whom must receive a State Department ID granting both physical and logical access.	Revise to read, "An Applicant provides two forms of identification from the list of acceptable documents included in the Form I-9, OMB No. 1115-0136, Employment Eligibility Verification *or equivalent national standard from the country of citizenship.* At least, one of the documents…*or national equivalent.*"

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
61	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E/T	Part 2, Section 5.2.1 (PIV Application and Approval), pgs 40-41	The process makes no provision or authorization for the use of electronic forms, in direct violation of the GPEA, E-Sign, and E-Gov legislation. Source documents can be scanned rather than photocopied, and an electronic form that accepts the digital signatures of the necessary officials will eliminate a bureaucratic administrative burden on agencies. Further, the applicant may have some type of (personal) digital signature, which is valid under E-Sign legislation.	Revise to read, "The PIV Requesting Official shall submit the PIV request and *either scanned or photocopied* copies of identity source documents for the Applicant *in electronic form* to…"
62	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E/T	Part 2, Section 5.2.1 (PIV Application and Approval), pg 41 (final subparagraph)	Visual inspection of identification documentation is, at best, a cursory proof of validity. This presumes that forged, stolen, modified identity source documents can be identified by visual inspection alone. Unless and until the identity source documents (e.g., I-9 documents) are sufficiently standardized and secured, visual inspection is futile. Further, it requires that the Registration Authority be knowledgeable and trained in this technique, and able to recognize a wide variety of identification. Finally, it assumes that the document was issued by a U.S. legal entity (e.g., Federal, state, local government or tribal council), is printed in English, and so forth.	Consider some form of verification other than visual inspection of the source identity documentation.
63	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 5.2.1 (PIV Application and Approval), pg 41 (final subparagraph)	This section introduces a contradiction to those portions of the standard (e.g., Part 2, Section 4.4.5) that mandate the use of a facial recognition biometric. The final sentence states, "The Registration may optionally also photograph the applicant for personalization of the PIV card." This is either a redundant use of photography or makes the collection of a facial biometric optional.	Revised the final sentence to read: "The Registration *shall* also photograph the applicant for personalization of the PIV card."

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
64	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E/T	Part 2, Table 5-2, pg 42	Position sensitive levels have existed within the Federal Government for many years (i.e., Critical-Sensitive, Critical-Nonsensitive, Sensitive, Nonsensitive) and are well documented and understood by those offices and personnel most likely to have to implement the PIV. Titles, such as Low, High, etc., are vague and open to interpretation, and should be left to the intellectually challenged.	Change the titles of Low, Moderate, etc., to titles that are already documented, understood, and in common use throughout the Federal government.
65	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E/T	Part 2, Section 5.2.1.3 (Overseas Foreign Workers), pg 42	This section directly contradicts the provisions of Part 1, Section 2.2.4, which vests this authority in the Department of State.	Select either the Department of State (preferred due to its mission and number of employees affected) or OMB, and standardize throughout the document.
66	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E/T	Part 2, Section 5.2.2 (PIV Card Issuance), pgs 42-43	What certificate/keys is the Issuing Authority using to sign the biometrics; and how is the Registration Authority securely transferring this data such that there is no possibility of tampering?	Recommend that the type and derivation of the Issuing and Registration Authorities digital signature/keys be specified
67	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 5.2.2 (PIV Card Issuance), pg 43 (third subparagraph)	A "database" containing PKI certificate information already exists as an integral part of the CA infrastructure. This information is, in turn, exported to the LDAP, AD, etc., directory for use. The directory may be replicated to a public directory for access via the FBCA, but is not a repository in this sense.	Review this proposed infrastructure vis-à-vis the typical PKI infrastructure and amend to eliminate the apparent duplication of effort.

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
68	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 5.2.3.1 (Architecture), pg 43	The requirement to participate in the hierarchical PKI for the Common Policy violates the provisions of both the Common Policy and the FBCA Certificate Policy (CP) that exempt existing, cross-certified CAs, particularly those operating at a higher assurance level. Further, since none of the currently cross-certified agency Principal CAs use the Common Policy, this requirement necessitates the establishment of another infrastructure, under a different policy.	Revise to read, "…shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI *or be otherwise cross-certified with the Federal Bridge CA at an equivalent or higher assurance level*."
69	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 5.2.3.2 (PKI Certificates), pg 43 (first subparagraph)	The requirement to participate in the id-CommonHW policy and the id-CommonAuth policy is unacceptable to the Department of State. This requirement violates the provisions of both the Common Policy and the FBCA CP exempting existing, cross-certified CAs; and it will necessitate the establishment of another infrastructure under a different policy by all currently cross-certified agency Principal CAs.	Revise to read, "…shall be issued under the…as defined in the X.509 Certificate Policy for the Common Policy Framework*, or be otherwise cross-certified with the Federal Bridge CA at an equivalent or higher assurance level*."
70	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 5.2.3.2.1 (X.509 Certificate Contents), pg 44	The requirement to participate in PKI under the Common Policy Framework is unacceptable to the Department of State. State Department established a business case over three years ago for a High Assurance PKI infrastructure to satisfy its unique operating environment and security needs. The Common Policy Framework is inadequate from both an operational and security point of view to meet those needs -- to include support for a worldwide PIV deployment.	Revise to read: "…based on the X.509 Certificate and CRL Profile for the Common Policy [PROF]*, or on the FBCA X.509 Certificate Policy for those agencies already cross certified under that policy at an equivalent or higher level of assurance.*

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
71	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Table 5-3, pg 45	This table reflects the PIV Authentication Key, the Digital Signature Key, and a Key Management Key, but does not reflect an Encryption Key, which is common in most PKI infrastructures. The use of an Encryption Key to provide privacy of communications in a Sensitive But Unclassified or Unclassified environment is a critical and integral part of most agency PKI.	Revised to add the Encryption Key with the appropriate expiration dates and algorithm standards.
72	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 5.2.3.5 (OCSP Status Responders), pg 45	This mandate requires the establishment of an infrastructure extension to those existing Principal CAs that chose, for business case reasons, not to implement an OCSP.	Revise to make this an optional requirement.
73	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 5.2.3.6 (Migration from Legacy PKIs), pg 46	The Comon Policy Framework does not support agency-specific requirements supported by valid, long established business cases. The Common Policy Framework provides only a Medium Assurance level, which is insufficient for some agencies (e.g., Department of State).	Revoke this requirement.
74	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 5.2.4.1 (Renewal), pg 46 (third subparagraph)	PKI policy and technology do not permit the export/import of keys between hardware cryptographic tokens. If the key management key functions similarly to the encryption key, then the key history can be migrated, but not the previous key.	Specify the derivation of the key management key, add the encryption key, and revise the second sentence as follows: If the PIV card supports the optional key management key, *the key history may be migrated* to the new PIV card. *In a like manner, the optional encryption key history may also be migrated to the new PIV card hardware token.*
75	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 5.2.4.2 (Re-issuance), pg 46 (second subparagraph)	There is no specification as to how long a PIV card shall remain valid. PKI certificates at the high assurance level are typically valid for 3 years, and it is recommended that this criteria be adopted.	Add the following as a second sentence: *PIV cards shall be valid for a period of three years from the date of issuance.*

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
76	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 5.2.4.2 (Re-issuance), pg 47 (final subparagraph)	The establishment of an 18-hour window for all revocations (except emergencies) is unacceptable. Agencies operating PKI at the High Assurance level have only a six hour window in which to revoke the PKI certificates. The revocation of the PIV card should mirror the standards for High and Medium Assurance levels outlined in the FBCA X.509 Certificate Policy. Further, the requirement to revoke certificates and cards and publish a CRL within one hour of notification is equally unrealistic. PKI policy establishes specific procedures that are both reasonable and suitable for all agency business cases, including those agencies with remote and overseas locations.	Revise the second sentence as follows: Where the card cannot be collected, normal *operating procedures shall mirror the equivalent standard for any PKI certificates stored on the PIV card, but in no case exceed 18 hours from the time of notification.* Delete the next three sentences, and revise the final sentence to read: *Agencies are required to have procedures in place to update all servers and publish a CRL within six hours of notification of compromise, loss, or improper issuance to a false identity.*
77	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	T	Part 2, Section 5.2.4.3 (PIV Update), pg 47 (second bullet)	This violates PKI policy and may not be technically possible. When a signed data element is changed in any way, the digital signature will reflect that a change has occurred and the data may be invalid. The CHUID must be resigned with a valid digital signature.	Revise the second bullet to read: "*Resign the CHUID with a new digital signature"*
78	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 5.2.5 (PIV Card Termination), pg 47	The various situations outlined in the bullet list overlook several high possible situations. First, a Federal employee may transfer to another agency, thereby requiring a different card. Second, a contractor works for multiple Federal agencies and/or transfers from one Federal contract to another. In both cases, should the old card be available to that individual as proof of identity to obtain a new card?	Add the following bullet: (1) *An employee transfers to a new parent Federal agency;* Also determine how contractors working multiple agencies or moving between valid Federal contracts should be handled.

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
79	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T/E	Part 2, Section 6.1.1 (Authentication using PIV Visual Credentials), pg 50 (second set of bullets)	This subparagraph indicates the Agency Name and Seal are optional, yet paragraph 4.1.4.1, pg 19, specifies that these elements are mandatory.	Review the requirement, determine if these data elements are mandatory or optional (preferred), and modify either paragraph 4.1.4.1 or 6.1.1 accordingly.
80	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 6.1.2 (Authentication using the PIV CHUID), pg 51 (second subparagraph)	This subparagraph states, "…there is no attempt to correlate the data and identifiers on the card with the actual cardholder." If this is, in fact, the case, it appears that anyone presenting an otherwise valid card could be granted physical access to Federal facilities. This implementation must be supported by human (i.e., guard) review of the credential against the cardholder as outlined in Section 6.1.1.	Review this subparagraph for the "sense" of the text.
81	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 6.1.3 (Authentication using PIV Biometric Credentials), pg 52 (first & second subparagraphs)	The requirements of these two subparagraphs appear redundant. Identity assurance is typically based on some use (or combined use) of three factors: something you know, something you have, and something you are -- in that order. Admittedly the combination of any two increases security, and the use of all three is the best solution. However, these paragraphs mandate the latter in all cases involving electronic verification.	Review these two subparagraphs with a view toward making the combined use of the PIN and biometric optional (I.e., an "either-or" situation). Further, reconsider the use of a PIN, vice password, for logical access control.
82	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Section 6.3.1 (Assumptions and Constraints), pg 57 (bullet list)	This subparagraph makes the assumption that the network connecting the cardholder to the information resource is not trusted. If this assumption were correct, that would automatically imply the the network on which the information resource was stored is also untrusted. This is not the case in most Federal IT networks.	Review these assumptions and either clarify the text or modify/delete the assumption.

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
83	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T/E	Part 2, Annex A, pg 59 (first subparagraph)	The second sentence directly links the accreditation of the PIV card to accreditation of information systems. This linkage is fallacious; the PIV card is a security mechanism that may or may not involve IT systems in some way.	Revise to read as a new third sentence: *Accreditation of the PIV Card system is similar, but may be performed by the senior security official in an agency rather than the information systems Designated Approving Authority.*
84	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T/E	Part 2, Annex A, pg 59 (first subparagraph)	The sixth sentence directly links the certification of the PIV card system to certification of information systems, and to NIST SP 800-37. Again, this linkage is fallacious.	Specify that NIST SP 800-37, while a useful guideline on certification in general, is not directly applicable to the certification of the PIV card system.
85	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Annex A, Section A.2.5 (Internal Auditing for PIV Card Management), pg 63	This paragraph mandates regular audit reviews conducted by a trusted third party without specifying the standard for a "regular audit" (e.g., every 10 years is regular), or for a "trusted third party" (e.g., an agency IG, and outside contractor, GSA, OMB, etc.).	Revise this paragraph to specify the requirements for regular audits and trusted third parties.
86	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	Part 2, Annex B, pg 64	This paragraph (Section B.1) and accompanying table (Table B-1) outline the requirements for Physical Access Control Systems (PACS), but the use of these standards is neither discussed nor mandated within the main document. Section B.2 and Table B-2 provide a similar discussion of existing E-Authentication requirements and guidelines without mandating implementation.	Modify the primary FIPS 201 document to mandate the implementation of these standards.
87	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/E	Part 2, Annex E, Section E.2, pgs 77-78	Not all acronyms appearing in the document are reflected in this listing.	Review the FIPS 201 for acronyms and include all in Section E.2

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
88	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	None; general comment	As with the preliminary draft, there is confusion between requirements and specifications for physical and logical access controls. A requirement, standard, or feature that works for one may not be suitable for the other. For example, biometrics for physical access control must reside in a database to support intra- and inter-agency interoperability, but the same is not true for logical access control because there are other requirements (e.g., having an account) that negate the need.	Review the FIPS 201 and clarify what requirements are for physical access control, what requirements are for logical access control, and what requirements are suitable for both.
89	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	None; general comment	The preliminary draft discussed three types of biometric "templates": image, minutiae, and pattern. That document and the subsequent Public Draft generally dismissed minutiae and patterns as not providing for interoperability. However, there was no discussion of hybrid uses such as that currently being fielded by the Department of State for logical access control (a combined minutiae-pattern technique). Given that no standard exists for any biometric and the fact that biometrics fall into Part 2 of the PIV implementation, it seems more logical to delay making a specification decision until further development and testing have been done.	Recommend that the specifications for the use of biometrics be delay and/or published as a separate NIST Special Publication.

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
90	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	None; general comment	The relationship between match-on-card and some unspecified database for the storage of biometric information is unclear. In some instances, match-on-card techniques are related to both logical and physical access control, however match-on-card provides no comparison to confirm identity only that the fingerprints on the card and those offered by the individual are the same. In other instances, interoperability and comparison are stressed--necessitating some off-card capability--but nothing is said about how that will be accomplished.	Recommend that the specifications for the use of biometrics be delay and/or published as a separate NIST Special Publication.
91	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	None; general comment	Based on review of all required data elements (as well as industry statements since release), it appears that the 32Kb card is now dead, and the 64Kb card will be just large enough to hold the required data elements and little else (e.g., PKI digital signature and encryption certificates, other biometrics, and other agency-specific data elements). Currently, there is no card on the market or coming to the market by 10/2005 that will satisfy the requirements, much less fulfill the testing and certification requirements of FIPS 140-1/-2/-3 and other standards.	None; this is a conundrum that will force waivers until such time as the FBCA--PIV infrastructure is established and functioning.

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
92	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G/T	None; general comment	FIPS 201 places undo reliance on the rapid completion of even a minimal background check using existing systems and assets. Currently, it takes days-weeks-months to complete the various levels of background checks, particularly for higher levels of assurance. Further, it places a heavy and new workload not only on Federal agencies, but also on state/local governments and private businesses (e.g., credit bureaus) who are responsible for providing the verification as an unfunded mandate.	None; this is a conundrum that will force waivers until such time as the FBCA--PIV infrastructure is established and functioning.
93	Department of State	Tin T. Cao, IRM/OPS/ITI/SI	G	None; general comment	As noted throughout this review, implementation of FIPS 201)and SP 800-73) will place a significant financial burden on all agencies, but particularly those that have already implemented PKI, biometrics, and smart cards. Depending upon the final standards and implementation time lines, many of these agencies will have to halt ongoing programs, retool and/or replace existing but newly installed physical and logical access control systems and techniques, and revisit all activities already implemented to implement the new systems.	FIPS 201 (and SP 800-73) must address the PKI-biometric-smart card replacement process from both a financial and implementation time line point-of-view. OMB must be prepared to work with those agencies that have begun fielding of systems that meet the intent of HSPD-12/FIPS 201/SP 800-73, if not the exact standards being proposed.