From: Mike.Parker@do.treas.gov
Subject: Comments on Public Draft FIPS 201
To: Draftfips201@nist.gov
Cc: Harry.Lee@do.treas.gov

MEMORANDUM FOR THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

FROM: Mike Parker

Deputy Chief Information Officer

Department of the Treasury

SUBJECT: FIPS PUB 201 Comments from the Department of the Treasury

The Department of the Treasury appreciates the opportunity to provide technical comments on the Public Draft of FIPS PUB 201. We fully appreciate the timeline in which the NIST team is working under to issue the Personal Identification Verification (PIV) standard as mandated by Homeland Security Presidential Directive-12 (HSPD-12).

The attached comments are intended to provide NIST with visibility into the Treasury-wide challenges anticipated in implementing FIPS PUB 201. These comments also request clarification and provide recommendations so that Treasury can meet the needs of our Bureaus with their diverse missions, while leveraging the investment Treasury has already made in common access card (Smart Card) technology for use by Treasury employees and contractors for both physical and logical access to Treasury-controlled facilities and information systems.

We hope that our comments prove helpful as NIST continues to support HSPD-12. In the meantime, should there be specific questions, please contact Trung Nguyen at 202-622-2583 or trung.nguyen@do.treas.gov.

Attachments (2)

<<COMMENTS ON FIPS PUB 201 PUBLIC DRAFT.doc>>
<<Treasury_Comments_121304_FINAL.xls>>


COMMENTS ON FIPS PUB 201 PUBLIC DRAFT.doc


Treasury_Comments_121304_FINAL.xls

COMMENTS ON THE PUBLIC DRAFT OF FIPS PUB 201, *FEDERAL PERSONAL IDENTITY VERIFICATION (PIV) STANDARD,* FOR REVIEW AND CONSIDERATION BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Submitted By:

U.S. Department of the Treasury

PURPOSE OF DOCUMENT

This document provides the U.S. Department of the Treasury's ("Treasury") high-level comments on the Public Draft of FIPS PUB 201, *Federal Personal Identity Verification (PIV) Standard,* for review and consideration by the National Institute of Standards and Technology (NIST) team working on the development of this standard.

OVERVIEW

Treasury would like to submit for consideration the following comments on the public draft of FIPS PUB 201. These comments are intended to help provide NIST with a true understanding of Treasury's concerns and areas where more explanation from NIST would provide needed clarity and guidance.

As part of our response, Treasury has aggregated 183 comments from the Treasury Bureaus and Departmental Offices using the template provided by NIST. These comments along with the narrative from this document should provide a feel for the current Treasury position. Any consideration and clarification from NIST on these comments and others received on FIPS PUB 201, will help to clarify Treasury's position and direction in support of complying with Homeland Security Presidential Directive-12 (HSPD-12).

Treasury supports the direction and intent of FIPS PUB 201; however, the comments included in this document will provide insight into a few high level challenges for all to overcome. These challenges include:

Major Concerns:

1. *Funding Implications*: The timing of the release of HSPD-12 does not allow for the funding of new initiatives in the FY05 and FY06 budget. It is the beginning of Q2 FY05 and it is difficult to identify and reallocate funds that are being used for other critical programs.

2. *Definition of Federal Facilities and Information Systems*: The anticipated guidance from OMB concerning applicability of FIPS PUB 201 and the definitions of federal facilities and federally controlled information systems will be essential to understanding the scope of FIPS PUB 201. The potential cost impact of a universally applied standard could be significant. Agencies operate a wide range of information systems and facilities, many having unique access controls based on the operations of the organization. Agency implementation plans will depend a great deal on this OMB clarification and guidance.

3. *Personal Privacy and Union Concerns:* Treasury has several unions that we deal with. One of the biggest concerns from the unions is privacy. To this end, the implication of storing biometric information and other personal information on a common identification card could create great concern for these organizations.

General Concerns:

4. *Marketplace Maturity and Product Availability:* In general, FIPS PUB 201 refers to some concepts and techniques that are technically possible but highly complex. This complexity may inadvertently delay the implementation of the PIV concept as demonstrated by current and previous Federal smart card programs.

5. *Graduated Migration Path*: FIPS PUB 201 needs to consider migration paths for legacy systems. This will ensure that risk mitigation factors are considered for legacy systems investments, reducing risks of implementation and business policies and practices.

6. *Existing Investment in Legacy Access Control Systems*: Treasury, like many other Federal Agencies, has sensitive operational activities for which robust access control systems have already been implemented. Some are even integrated into production environments. Though Treasury and its Bureaus seek compliance with FIPS PUB 201 and its goals; it is recommended that there will be transition periods that will:

    a) Recognize the legitimate need for dual systems while legacy systems are replaced or re-engineered;
    b) Cross multiple fiscal years;
    c) Have minimal impact upon existing operations and services; and
    d) Give agencies flexibility as to migration strategy and timelines.

7. *Centralized Card Issuance:* FIPS PUB 201 seems to be geared towards local issuance of identification cards which could unnecessarily increase the cost of operation for agencies that have a widely dispersed population. Card issuance for these agencies could be handled through an equally effective local proofing process coupled with a centralized card production facility. Agencies should be able to conduct cost benefit analysis to determine best approach.

8. *PIV Appearance Uniformity:* There are only generalizations about the card topology. This ambiguity will lead to varying levels of compliance as each agency interprets the standard in a manner which suits its individual needs. FIPS PUB 201 defines minimums for font sizes. This should be strengthened to limit the ability to determine agency specific font sizes. There also appears to be no provision for the use of a background color or graphic. If this is not to be allowed it should be stated.

9. *Imposed Sensitivity Designations:* With the introduction of position sensitivity determinations and associated background investigations, the roles and responsibilities of OPM have become blurred. The background investigations associated with the proposed levels of sensitivity do not seem to coincide with current guidance from OPM. It appears inconsistent with the intent of HSPD-12 for FIPS PUB 201 to impose additional implementation guidance beyond that issued by OPM concerning position sensitivity determinations. It should also be noted that FIPS PUB 201 does not appear to coincide with the requirements of FIPS PUB 199, whereby FIPS PUB 201 imposes four levels of sensitivity and FIPS PUB 199 mandates three levels and permits agencies to establish additional levels.

10. *Identity Credential Issuance:* By requiring a completed background investigation prior to issuance of a final Identity Credential, FIPS PUB 201 imposes an unnecessarily strict procedure as compared to the current accepted practices for other types of accesses, such as those concerning interim and final personnel security clearances. A final Identity Credential should be made available to all employees and contractors immediately upon verification of their personal identity and not wait for the completion of a potentially lengthy background investigation. An effective policy could be for issuance of the final Identity Credential once the Registration Authority verifies the Applicant's source identity documents with the agency issuing those documents. Additionally, clarification is needed concerning the associated limitations of authority, responsibility, rights, and privileges of the employee during the period they are waiting for the completion of the background investigation and, in accordance with FIPS 201, are being treated as a "visitor".

11. *Physical Access Control Systems:* NIST has stated several times that it is not dictating the type of physical access control systems for agencies to use, but in reality NIST is dictating the technologies and process to be employed by any physical access system, which in turn has a direct affect on the availability of compliant systems.

12. *Certification and Accreditation:* The requirement for certification and accreditation specified in FIPS PUB 201 is going to prove to be a monumental task for all agencies implementing the systems required to meets FIPS PUB 201. The C&A process is a lengthy and costly one that should be discussed in great detail. Agencies will have to determine the resources and funding necessary to meet the requirement in an unrealistic timeframe. Guidance is required to identify the appropriate references, time frame and tools available to meet this requirement.

13. *Implication of Mandatory FIPS*: Because Federal Information Processing Standards are mandatory and cannot be waived, it is unclear what status non-compliant practices will have on the effective date of FIPS PUB 201.

Thank you for taking our comments into consideration. If you have any questions, please contact Trung Nguyen at (202) 622-2583 or trung.nguyen@do.treas.gov.

Cmt #	Org.	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	Department of the Treasury	Trung Nguyen	G	Overall	The standard does not put any emphasis on the overall effect of this type of standard. There are three major aspects that is not discussed; one resources that it will take to implement and carry out the standard, two this is a un-funded mandate, and three the enterprise systems that are already in place.	
2	Department of the Treasury	Trung Nguyen	G	Overall	Within the standard it states the various systems and how they will interact with each other. One issue with the interaction of the systems is there is no disconnect between the physical access control system and the logical access systems. This could create possible vulnerabilities. Within Figure 3-1 the relationships between the systems needs to be clarified.	
3	Department of the Treasury	Trung Nguyen	G	Overall	There is a presentation on the NIST web site: Personal Identity Verification for Federal Employees and Contractor. William Barker is listed as the POC. Page 2 provides a Scope of PIV Subscribers. This level of detail would add value to 201.	Add a description of Federal Contractors and employees using sited presentation.
4	Department of the Treasury	Trung Nguyen	G	Overall	The requirements concerning personnel security should be coordinated with OPM. OPM is delegated authority to make and implement policy concerning security requirements of "people", much of which has been tested in court. Changes to position risk, investigations, etc., would be expected to require public notice and comment through the Federal Register. Moreover, OPM and DOD have been collaborating on centralizing investigation information (CVS, DCII, and SII systems) and creating one repository. This has not happened according to early plans, nor is an expected rollout date addressed in FIPS 201.	
5	Department of the Treasury	Trung Nguyen	G	Overall	No section on integration and interoperability of card readers for physical access. Industry is currently highly proprietary.	
6	Department of the Treasury	Trung Nguyen	G	Overall	Sure to be significant: National Treasury Employee Union interest regarding privacy implications with the biometrics portion of the concept. {Operational Assurance}	
7	Department of the Treasury	Trung Nguyen	G	Overall	How will the notice, personal information and privacy rights of employees and contractors be protected across agencies and during exchanges? Are specific assurances to be given to contractors and their companies? Will there be independent oversight or external enforcement?	

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

Cmt #	Org.	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	Department of the Treasury	Trung Nguyen	G	Overall	Market research and case studies of actual deployments indicate that the reliability, quality and acceptance of smart card and biometric technologies have not risen to a level of maturity that qualifies for widespread usage. While the science and technologies are advancing rapidly, it does not appear that the commercial sector presently provides multiple sources of a mature product offering in biometric technology to support large scale general purpose applications at the quality assurance levels required for production operations, commercial use or interoperability.	
9	Department of the Treasury	Trung Nguyen	G	Overall	Agency use policies may need to be annotated to prescribe responsibilities and standards for the life cycle management of digital signatures and encrypted data files created by employees and contractors especially in the event of changes in status such as retirement, termination, promotion or transfer to a different division. What restrictions will apply to the recovery, access or deletion of encrypted data files subsequent to a change in status?	
10	Department of the Treasury	Trung Nguyen	G	Overall	What assurances for privacy and identity data protection will all employees and contractors be afforded with the implementation of this standard?	
11	Department of the Treasury	Trung Nguyen	G	Overall	What constitutes agency due diligence with respect to he card holder's rights of privacy and the protection of personal data should be explicitly stated in the standard. The card holders' intended role, rights and responsibility in the lifecycle management of their personal data and credentials should be clearly stated as guidance for the agency and the card holders to ensure consistent application across agencies..	
12	Department of the Treasury	Trung Nguyen	G	Overall	Will service level metrics or customer services standards be prescribed for agencies to assure subscribers that the card issuance, identity verification and customer related services will be handled in a timely and professional manner? A federal service level management standard should be proposed to establish a minimally acceptable standard of performance.	Service level agreements should be prescribed to ensure that personal identity verification is actually accomplished in a timely manner from a customer-centric perspective comparable to the e-Gov and PMA initiatives.

Cmt #	Org.	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 the Treasury	Trung Nguyen	G	Overall	Was it intended that employees, contractors or supervisors be able to receive information about the status of their request for card issuance or review the data collected to verify their identity for accuracy as a routine service capability? If so, will a uniform service capability be prescribed?	
14	Department of the Treasury	Trung Nguyen	G	Overall	Will service level agreements (SLAs) or customer services standards be prescribed for agencies to assure subscribers that the card issuance, identity verification and customer related support services will be handled in a timely and professional manner? Will employees or contractors be able to request information about the status of credentials or review the data collected to verify their identity for accuracy? A federal service level management standard should be proposed to establish a uniform and minimally acceptable standard of service.	
15	Department of the Treasury	Trung Nguyen	G	Overall	Federal efforts to improve security and identity management have established a number of initiatives and working groups with overlapping scope and conflicting guidance. Given the constraints upon resources, a clear understanding of roles, responsibilities and objectives is needed to comply with the aggressive schedules and timelines established to achieve the critical improvement in our security posture. Guidance should be provided to reconcile inconsistencies and conflicts in the schedule and objectives of competing and complementary activities.	Prescribe use of existing standards and policies such as SP 800-36, SP 800-37, SP 800-63 and others.
16	Department of the Treasury	Trung Nguyen	G	Overall	In an effort to increase the assurance of personal identity, it is equally or more important that we certainly do not create a security infrastructure that is a more vulnerable or attractive target to terrorists and attackers than the existing systems that are being modified or replaced. In order to share common data and reduce costs, it is critical that data privacy and data protection controls do not put potentially more useful information in the hands of terrorist and attackers in the event of a security breach. This standard does not address how agencies must protect and secure shared privacy and identity data about employs and contractors.	The standard should prescribe a uniform implementation strategy to clarify the desired outcomes, reduce the opportunities to increase costs or select options that compromise interoperability.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
17	Department of the Treasury	Trung Nguyen	G	Overall	It is important that the contact and contactless cards and readers used for physical and logical access be compatible. It is unclear from the specifications and referenced standards that this is the desired outcome. The cards and readers that are specified for physical access should be capable of meeting requirements for logical access as well.	
18	Department of the Treasury	Trung Nguyen	G	Overall	How will prescribed physical access controls apply to federal staff and contractors working in buildings or facilities that are not federally-controlled or federally-owned?	
19	Department of the Treasury	Trung Nguyen	G	Overall	With all the words that are being utilized interchangeably throughout the document, the most confusing is the process of proofing the individual is to provide a level of assurance that the individual is indeed who the say they are. Where as a credit check may be done to determine the trustworthiness of said individual. Is it the intent of the standard to provide a level of assurance that the individual is who they say they are and that they are trustworthy? Or is it to provide a level of assurance that they are who they say they are? The utilization of these words within the document is so loosely based that it creates confusion towards what the standard is trying to accomplish.	Provide a clearer definition of the two terms and explain how they work together in the process. Discuss both in the context of the topic and be consistent in the necessity of how one is used. Is trustworthiness necessary for validating an identity or is it to determine someone, who's identity has been established worthy of hold a specific position. This would pertain to the requirement of credit checks.
20	Department of the Treasury	Trung Nguyen	G	Overall	Seems to be gear more too local issuance of identification cards than one with the flexibility to provide for the numerous employees and contractors located in remote locations that may not be cost effective to host a local issuance process. This approach could un-necessarily increase the cost of operation for agencies that have a widely dispersed population and one that could be handled through an effective local proofing process coupled with a centralized card production facility.	Provide for local face to face proofing and centralized card production.

Cmt #	Org.	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		Trung Nguyen	G	PIV-I	PIV-I is lacking an extreme amount of detail. What about data archival requirements - IAW NARA, for how long should the archives be stored, etc? Audit requirements? What about lifecycle mangement of cards, especially with respect to digital certificate maintenance when certificates expire, are revoked, suspended etc.? How does PIV I registration process scale to accomodate larger or more geographically diverse agencies with greater challenges? How are Registration Authorities and other authoritative roles vetted themselves - how are they "trusted" to issue credentials for others? What about "M of N" procedures in the vetting process that would require collusion to subvert?	
22	Department of the Treasury	Trung Nguyen	G	PIV I	In PIV I there is only the standardization of some of the business processes of issuing a credential, this section does nothing to ensure the validate of the issuer, provide a strong identity card or even standardize the ID card. There is not effort to ensure the issuance of a standardize government identification card which has the ability to be verified as being issued by a accredited issuer. There is no means to provide an ID that has employed any anti-counterfeiting measures. There is not specified means of authenticating electronically. These items are listed as control objectives of PIV I but never listed or explain within PIV I. Without the requirement for these control objectives and the re-issuance of a STANDARDIZE PIV card how is this providing anything stronger than what is currently in place?	State upfront how this will meet HSPD 12 if it does.
23	Department of the Treasury	Trung Nguyen	G	PIV-II	Strong requirements are needed regarding card management as it relates to the collection, storage, access to and disposal of this extremely sensitive information, that if compromised/stolen can have adverse consequences to the individual the information is about. Should the card management be handled by contractors or should it be an inherently government position. {Privacy}	
24	Department of the Treasury	Trung Nguyen	T	Section 3, pg. iv	Define an official accreditation process.	per NIST 800-37
25	Department of the Treasury	Trung Nguyen	G	Section 6, pg. v	It is not clear what is meant by the term "federally controlled information system" nor how it would be determined. Some federally-owned applications are hosted on commercially controlled, owned and operated systems.	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
26	Department of the Treasury	Trung Nguyen	G	Section 8, pg. v	What standards and controls will be applied to the certification of interim issuers of identity credentials until a government-wide PIV-II accreditation process is established? Without standards and enforcement criteria it may prove difficult to establish a reliable trust model within or across agencies.	
27	Department of the Treasury	Trung Nguyen	T	Section 8 pg. v	An interoperability standards and testing service will should be established to reduce the need for agency investments in testing and validating interoperability standards equipment and integration schemes. Certification of tested equipment, software and related technology will mitigate the aggressive schedule for deployment.	
28	Department of the Treasury	Trung Nguyen	G	Section 8, pg. v	Further guidance should be provided about reciprocity and assurance in investigations. Currently, agencies may reciprocally accept other agency background investigations if the criteria is the same as theirs. However differences exist in investigations and processing of them due to agency's unique business and nexus of issue, (i.e. FMS heavily weights financial issues). This may raise issues in ability of agency to grant access to systems to employees of other agencies where factors are not weighted the same. Agencies will need to have an assurance that the investigation of the "visitor" meets their weighted standards before granting access to systems and assets.	

Cmt #	Org.	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		Trung Nguyen	G	Paragraph 10, first bullet, pg. vi	"Assurance provided by the parent organization that the person to be issued the credential has been correctly identified." This qualification effectively abrogates the very first criteria in HSPD-12 for a Secure and reliable form of identification. The Secretary of Commerce is charged with defining the procedures for verifying employee identity. Without a single government-wide standard for this first, foundational step, FIPS 201 will do nothing to change the current stumbling block to interoperability, that of one agency not trusting the process another uses to issue credentials. In fact, this step is not the responsibility of the Applicant's parent organization (the PIV Requesting Official and the Authorizing Official), but rather, the Registration Authority that does the background investigation and the Issuing Authority that crosschecks the applicant with the results of the investigation (per Sections 2.2.1 and 2.3).	FIPS 201 must define a single government-wide standard for verifying employee identity.
30	Department of the Treasury	Trung Nguyen	T	Section 6, pg. v Section 1.2, pg. 1 Section 2.1 bullet point 6, pg. 4	Define a Federally controlled information system? How does this term relate to major applications and minor applications? Are minor applications subject to this standard? Is a federally owned information system different than a federally controlled one? A clear definition of "Federally controlled Information Systems" is required. Are all systems owned by the Federal Government to fall under this definition? Are only system designated above a certain risk level subject to this? In addition when in the life cycle of the system does it fall under these requirements?	Use terms the community is already familiar with such as major application. HSPD indicates that each Department must determine when and where to apply this standard. State this up front.
31	Department of the Treasury	Trung Nguyen	G	Section 2	There are no specify minimum qualifications/position sensitivity levels for the PIV Requesting Official, PIV Authorizing Official, PIV Registration Authority, and PIV Issuing Authority which address identity and suitability.	FIPS 201 should specify minimum qualifications/position sensitivity levels for the PIV Requesting Official, PIV Authorizing Official, PIV Registration Authority, and PIV Issuing Authority which address identity and suitability.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
32	Department of the Treasury	Trung Nguyen	G	Section 2	FIPS 201 provides a standard for personal identity background checks for the various position sensitivity levels that are intended to provide given level of assurance of the person's identity. It is important to note that the PIV addresses identity and does not appear to address or imply suitability. Expiration date is required, but FIPS 201 does not state the maximum period for which a card can be valid. Standards for periodic background check updates should be referenced or established. And proofing for current employees must only have the most recent background check on file - what if the most recent check is 25 years old? This limits reciprocity between agencies, ability to 'transfer' credentials, and does not allow position sensitivity levels to be mapped to FIPS 199 categorization levels.	
33	Department of the Treasury	Trung Nguyen	E	Section 2.1 pg. 4	You state in the 5th bullet that systems shall "Implement an identity credentials that support rapid electronic authentication". Is this for systems that are currently in place or new proposed systems?	Provide clarity for this statement. If it is to deal with current systems please provide technical guidance or clarity for this item. Please provide a definition of electronically validated as it applies to PIV I.
34	Department of the Treasury	Trung Nguyen		Section 2.1, third bullet, pg. 4	"Issue credential through systems and providers whose reliability has been established by the agency and so documented and approved in writing." Here again the responsibility to establish uniform processes and standards is being abrogated. In order to ensure cross-Agency trust, the process for establishing and verifying the reliability of both systems (hardware, software, and processes) and providers (the personnel operating and administering the system) must be uniform across all of government; it cannot be left up to each agency. And while Appendix A does provide a guide for qualifying hardware and software, FIPS 201 is completely silent on how to ensure the quality and reliability of the most important part of the chain of trust – the personnel who will be charged with operating these systems.	
35	Department of the Treasury	Trung Nguyen	G	Section 2.2, pg. 4	The guidance states that one individual shall not assume more than one role in this process. Then in the paragraphs that follows the guidance switches between individuals and entities performing the tasks.	The guidance should be consistent either individuals or entities, preferably entities or offices performing the tasks.

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

Cmt #	Org.	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 the Treasury	Trung Nguyen		Section 2.2, pg. 4	The internal controls and separation of duties prescribed for the identity proofing and registration process should be described more definitively to clarify the boundaries of the roles and responsibilities of the individuals and the entities involved in the process.	
37		Trung Nguyen	T	Section 2.2, p.5	Somewhere it should be noted that the PIV Authorizing Official and the PIV Registration Authority CAN be the same person. In practice, these roles inherit similar responsibilities that could be performed by a single entity to reduce administrative complexity.	
38		Trung Nguyen	T	Section 2.2, p.5	Is the PIV Issuing Authority envisioned to be a Certification Authority in the case of issuing digital certificates? In this case, a physical and logical issuing authority can be vastly different entities (the former being a person) with vastly different obligations in the PIV process. Suggested that some clarification be made to avoid confusion. Also, in many cases the physical issuing authority can also be the authorizing official and/or registration authority.	
39	Department of the Treasury	Trung Nguyen	G	Section 2.2, pg. 7	Identity Proofing and Registration of New Employees and Contractors: The document requires that paperwork and documentation be provided the Registration Authority, Authorizing Official and Issuing Authority. Although there is a need to verify identity, the fingerprinting process done up front with new employees verifies they are who they say that are. Requirements in this section seem to be excessive and guarantee that the entire process is slowed down and issuance of ID media to a new employee will be delayed. The requirement of two photo ID's as verification of identity is not practicable when applications are submitted from a distance and interviews are done via telephone and face to face is not done until well into the hiring process. {Physical Security}	
40	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 5	This sections discusses the forms of identifications and photocopies being produced for the PIV. The guidance does not state what the retention schedule of the documents will be. Also the guidance only addresses if the documents are approved not disapproved.	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
41	Department of the Treasury	Trung Nguyen	G	Section 2.2.1 pg. 6	It is stated that you will collect all of the fingerprints from each applicant as described in section 4.4.3 (which is not a requirement to satisfy PIV 1 and HSPD 12). If this is a requirement of PIV 1 shouldn't the technical information be contained in PIV 1 as to reduce confusion and provide guidance?	Either remove this requirement or provide clear guidance to the technical and processes necessary to meet this requirement in PIV 1.
42	Department of the Treasury	Trung Nguyen	T	Section 2.2.1, pg. 5	2nd Paragraph: Has a legal opinion been obtained from INS on references pertaining to the I-9? The Immigration Act of 1990 added a requirement that employers could not discriminate against employees by requesting more or different documents. Therefore the statement in this paragraph that at least one of the documents shall be a valid State or Federal Government issued picture ID may be illegal. Also the sole intent of the I-9 is for employment verification to ensure that employers are not hiring illegal immigrants. It was not meant to be a source for verifying identify. Recommend staying away from any references to the I-9, but rather go with a listing of documents that are appropriate for verifying identity. Rationale is that the I-9 is very restrictive as to the uses and the fact that agencies cannot dictate to an applicant the documents that they should provide. {Policy}	Develop a clear and concise policy for validating identity which is separate and apart from the employment verification process as required by the Immigration Reform Act of 1986 (for the I-9 process.) Recommend criteria contains two source documents, one of which would be government issued picture ID media.
43	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 5	1st Paragraph under the Tables: In IRS, NBIC would become the Registration Authority who conducts the background investigations. However, employees and contractors route their background investigation forms through BI coordinators and COTRs who are not a part of NBIC. IRS hires applicants and contractors all over the US, Puerto Rico, and Internationally, where no NBIC personnel, BI Coordinators or COTRs are located. We would not have the staff to be able to personally review documents and to meet face to face with all employees and contractors. Also, IRS does not have fingerprinting facilities in all locations and relies upon individual law enforcement agencies to fingerprint employees and contractors. {Policy}	Recommend giving agencies authority to delegate responsibilities for visually inspecting the identity source documents and to use outside sources for fingerprinting. A policy would need to be written on how to handle situations where applicants need to be fingerprinted by outside law enforcement agencies.
44	Department of the Treasury	Trung Nguyen	T	Section 2.2.1, pg. 5	"The PIV Requesting Official shall ..the PIV request and photocopies of identity source document ..." The documents require safe transport because copies can be altered and copied. {Privacy}	insert some language regarding how the document copies should be transported, stored and access controlled.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
45	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 5-7	In part, the guidance states that the "registration authority" shall visually inspect the identification documents and authenticate them as being acceptable. Visual inspection appears to be inadequate with the prevalence of forged documents such as drivers licenses, social security cards, etc. Should the registration authority go to the source point of the document, State Motor Vehicle Department, to ensure the document was issued by the State? The other aspect is that the Registration Authority must become an expert in the documentation being presented to determine if it is authentic. This could mean being familiar with all State issued credentials such as drivers licenses.	
46	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 6	In the tables set forth in this section the Sensitivity Levels to do not match OPM's. In Table 2-2 Sensitivity Level 4 states that an LBI or BI would be conducted, if this is a Critical (Vital National Asset - Critical Infrastructure) Position then OPM requires a Single Scope Background Investigation (SSBI) be completed. In this section there is no mention that these are the minimum levels of background investigations that can be completed. the bureaus are very diverse organizations and multiple levels of investigations are completed, I.e. some are not listed in the table and they are higher than they propose for the sensitivity levels.	
47	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 5	Section 2.2.1 states that the Applicant provides two forms of identification to the PIV Registration Authority. Then it states that the Applicant provides a completed background information forn to the Registration Authority and appears in person to provide the same identity source documents provided earlier to the PIV Requesting Official.	Clarify the identity proofing process outlined in the draft FIPS PUB 201, and add a diagram of the process.
48		Trung Nguyen	T	2.2.1, p.6, final paragraph	Is the Issuing Authority a person or a system? Differentiate - this is confusing.	
49	Department of the Treasury	Trung Nguyen		Section 2.2.1, pg. 5	The employment status assigned to each applicant should be added to the profile. Whether or not a applicant is a federal employee, contractor employee or foreign national may be critical for authentication or authorization purposes especially with respect to logical access security controls.	

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

Cmt #	Org.	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 the Treasury	Trung Nguyen		Section 2.2.1, pg. 7	The recordkeeping responsibilities of the Registration Authority requires the maintenance, protection and management of identity source documents. This requirement may significantly increase the amount of paper and the cost of storing duplicate data on employees and additional data on contractors for prescribed periods of time. Records and document management implications may be significant.	
51	Department of the Treasury	Trung Nguyen	G	Table 2-2, pg. 6	This appears to require anyone with access to a Vital National Asset – Critical Infrastructure – to have at the least an LBI. Is this the intent? Additional guidance states that copies of several sensitive (privacy related) documents are to be maintained by the Registration Authority. Is it the intent to create a "paper blizzard" of documentation for each government employee and contractor? Should this document suggest that a digital repository of required documents is adequate? Should this digital repository (if adopted) be accessible by other registration authorities such as in the case of an employee transferring from one agency to another?	Need specifics
52	Department of the Treasury	Trung Nguyen	G G	Section 2.2.1, pg. 6 Table 2-2, pg. 6	Clarification is needed for the term "successful completion of the appropriate background check". Does NIST really mean adjudicated background investigation? Can an agency define background investigation? (i.e. FMS completes preliminary screening-does this suffice for "investigation"?) FMS background check requirements are more stringent in regards to types of investigations conducted.	Restate these as the minimum that can be adjusted by agencies to meet more stringent requirements.
53	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 6	Further guidance should be provided about position risk levels affected by this requirement. Currently, personnel security guidelines addressed in FIPS 201 do not reflect the OPM standard guidelines for position risk designations. OPM identifies public trust positions (low, moderate, height) and national security/security clearance positions (non sensitive, non critical sensitive, critical sensitive and special sensitive) and the correct investigations for each risk level.	

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

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
54	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 6	Table 2-1: The Form I-9 is not intended to collect information for a background investigation. It does not contain the necessary information needed for a background investigation nor does it contain the Authorizations for Release of Information. The I-9 should not be used for personnel security background investigation purposes. IRS uses the SF-85P for all position risk sensitivity levels on contractors; the SF85 for low risk employees, the SF85P for moderate and high risk employees; and the SF-86 for national security. {Policy}	Recommend change to show use of the Form SF-85, Questionnaire for Non-sensitive Positions or equivalent for Level 1 - low risk; SF-85P for level 2 and 3 - moderate and high; and SF-86 for level 4 - Critical
55	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 6	Tables 2-1 & 2-2: Hopefully, the levels indicated on both charts refer to the minimum level of investigation needed to be conducted in order to issue the ID media. We at IRS conduct NACI for low risk, LBI for moderate, and BI for high risk; on contractors we conduct a Basic (NAC equivalent plus tax checks); moderate a NACLC; and high a BI. {Policy}	Reference should be made in these sections that the types of investigations identified are the minimum level required in order to process and that agencies retain the right to investigate at higher levels, but not less than the minimum standard.
56	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 6	2nd paragraph under the tables: It requires that a successful completion of a background investigation is required before issuance of a PIV. In IRS, we approve employees for access based on successful completion of a fingerprint screening before EOD and contractors must pass an interim determination of a fingerprint and tax check for unescorted access. Completion of a background investigation before issuance of a PIV would impact successful business measures. {Policy}	Allow agencies to implement interim procedures while background investigation is being completed.
57	Department of the Treasury	Trung Nguyen	G	Section 2.2.1, pg. 6	1st Paragraph under the Tables: In IRS, NBIC would become the Registration Authority who conducts the background investigations. However, employees and contractors route their background investigation forms through BI coordinators and COTRs who are not a part of NBIC. IRS hires applicants and contractors all over the US, Puerto Rico, and Internationally, where no NBIC personnel, BI Coordinators or COTRs are located. We would not have the staff to be able to personally review documents and to meet face to face with all employees and contractors. Also, IRS does not have fingerprinting facilities in all locations and relies upon individual law enforcement agencies to fingerprint employees and contractors. {Policy}	Recommend giving agencies authority to delegate responsibilities for visually inspecting the identity source documents and to use outside sources for fingerprinting. A policy would need to be written on how to handle situations where applicants need to be fingerprinted by outside law enforcement agencies.

Cmt #	Org.	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	Department of the Treasury	Trung Nguyen	G	Sections 2.2.1 & 2.2.4, pgs. 6-7	In both sections it states that identity credentials will not be issued to employees until the background investigation is complete. Due to the length of time that a background investigation takes to be completed, I.e. 18 to 24 months, this does not seem to be an effective process.	
59	Department of the Treasury	Trung Nguyen	G	Sections 2.2.1 & 2.3, pg. 7	In both sections it states that copies of the completed PIV requests will be kept. This will generate multiple files and numerous paper documents that will need stored. Is the intent to maintain this electronically or paper form? If the intent is paper format then this would conflict with the Government Paperwork Elimination Act (GPEA)	
60		Trung Nguyen		Section 2.2.1, second paragraph, pg. 5	"The PIV Authorizing Official shall submit the PIV request and photocopies of identity source documents..." Specifically requiring photocopies prevents the use of digital copies, signed e-mails, and document management systems as envisioned by the e-gov program.	
61		Trung Nguyen		Section 2.2.1, fourth paragraph, pg. 6	"In addition, the Applicant shall appear in person and provide two forms of identity source documents provided earlier to the PIV Requesting Official." It appears the intention is for the Applicant to present the same source documents to both the Requesting Official and the Registration Authority.	Recommend rewording the sentence to read "In addition, the Applicant shall appear in person and provide the two identity source documents which were provided earlier to the PIV Requesting Official."
62		Trung Nguyen		Section 2.2.1, fourth paragraph, pg. 6	"The Registration Authority shall visually inspect the identification documents and authenticate them as being acceptable."	Recommend providing guidance or methodology for how the Registration Authority is to do this, which both weakens the chain of trust and erodes cross-agency confidence in the issuance process. As stated in the opening paragraph of this section "The paper-based source documents by themselves provide very weak assurance of identify." Without a standard process for verifying them they remain very weak, undermining the validity of the credential that is being applied for.

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

Cmt #	Org.	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		Trung Nguyen		Section 2.2.1, fourth paragraph, pg. 6	"The Registration Authority shall conduct the appropriate background check..." Background checks are performed by the Office of Personnel Management or the Defense Security Service. Is the intent that the Applicant's sponsoring agency have a Registration Authority, who sends the collected paperwork and fingerprints to OPM/DSS for the investigation, or are these two agencies (OPM and DSS) to be the Registration Authority for the federal government?	
64	Department of the Treasury	Trung Nguyen	G	Section 2.2.2, pg. 7	The guidance states that when issuing or re-issuing identity credentials to current employees, the identity proofing in Section 2.2..1 shall be followed except the background checks. Once PIV II is put in place there will need to be a mass re-issuance of ID cards to all employees due to mandatory requirements. Agencies have career employees, 10, 20, 30 years of service, that have current ID cards issued to them. This process would require agencies to ask them to validate who they are with two forms of Identification from the I-9 Form. Also with each card having an expiration date agencies would be required to go through this process upon each mass re-issuance per this guidance.	
65	Department of the Treasury	Trung Nguyen	E	Section 2.2.3, pg. 7	Long-tem	Should be term.
66	Department of the Treasury	Trung Nguyen	G	Section 2.2.3, pg. 7	This section states a long-term credential can not be issued until the background investigation is complete. Long-term is not defined, some agencies have long-term visitor badges, I.e. 6 month badge.	Long-term should be defined.
67	Department of the Treasury	Trung Nguyen	T	Section 2.2.3, pg. 7	Visitors are required to be escorted and are not eligible for even an email account. Is this the intent?	End the sentence with ...shall not be issued long-term identity credentials.
68	Department of the Treasury	Trung Nguyen	E/G	Section 2.2.3, pg. 7	While the intent seems to be good, the practicality does not appear to be addressed. The language is too restrictive. Allow agencies to determine how and if "provisional access and provisional (local) credentials" may be issued since some background investigation may take up to 12 to 18 months to complete.	

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

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
69	Department of the Treasury	Trung Nguyen	G G	Section 2.2.3, pg. 7 Section 2.2.2, pg. 7	Clarification is needed for process to handle new and existing employee and contractors who do not have a completed background investigation. FIPS 201 states they shall be treated according to visitor procedures, which require escorts, etc. This is not realistic. Background investigations by OPM can take up to two (2) years to complete. Need to make sure employees current clearance is within time limits for the particular clearance, i.e., it has not expired.	...if the results of the most recent previous check are on file, is current for the level of risk and can be...
70	Department of the Treasury	Trung Nguyen	E	Section 2.2.3, pg. 7	Replace long-tem.	Should be: long-term
71	Department of the Treasury	Trung Nguyen	G	Section 2.2.3, pg. 7	NIST FIPS PUB 201 will require that no employee or contractor be issues PERMANENT identification until a background investigation has been COMPLETED. Until that time employees and contractors can only be issued VISITOR badges. Some VISITOR badges are ESCORT ONLY. In preparation for the filing season many locations employee seasonal employees and some of these employees are brought on duty prior to the completion of the background investigation. Implementation of PIV-1 under FIPS 201 will require that this practice stop. All employees and contractors must have a competed background investigation prior to issuance of permanent credentials	Propose some criteria short of full investigation that would not require escort only access. For instance, some individuals will not require access to sensitive information but would require frequent access to facilities that could become routine in nature (cleaning crews, etc..) Some Criteria that would allow un escorted access but restrictions as to the type of data access.
72	Department of the Treasury	Trung Nguyen	G	Section 2.2.3, pg. 7	Are there any provisions for 'seasonal' workers {Policy}	Define temp badge process
73	Department of the Treasury	Trung Nguyen		Section 2.2.4, pg. 7	Restricting the issuance of long-term identity credentials to an applicant until the required credential verification process is completed is not practical in many situations. Most notably, senior staff awaiting confirmation or clearance before assuming duties after appointment. In routine cases, visitor status does not entitle an applicant to have access to or use information systems. In some cases, escorts may be required for extended time periods.	

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

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
74	Department of the Treasury	Trung Nguyen		Section 2.2.4, pg. 7	Is he State Department approved method available for review? How may information regarding this process be obtained?	
75	Department of the Treasury	Trung Nguyen	T	Section 2.3, pg. 7	How does the IA confirm the validity of the PIV request?	
76	Department of the Treasury	Trung Nguyen	T	Section 2.3, pg. 7	There is a significant overlap on the documentation required by the RA and the IA. Is this necessary?	
77	Department of the Treasury	Trung Nguyen	E	Section 2.3, pg. 7	Case issue with: I.e	Should be: i.e.
78	Department of the Treasury	Trung Nguyen		Section 2.2.4, pg. 7	What is the definition of long-term and what restrictions on physical and logical access are intended?	A provisional status credential should be issued to meet prescribed restrictions. Neither employees nor contractors physical access to facilities or logical access to information systems should be denied until a background investigation is completed.
79	Department of the Treasury	Trung Nguyen	G	Section 2.3, pg. 7	Will the completed and formally authorized PIV request replace the completed and signed PIV request maintained by the Registration Authority? {Privacy}	To maintain the most current information regarding an Applicant - the Registration Authority completed & signed PIV request should be replaced with the completed and formally authorized PIV request and the previous request destroyed.
80	Department of the Treasury	Trung Nguyen	G	Section 2.3, pg. 7	Identity Credential Issuance: The document requires that paperwork and documentation be provided the Registration Authority, Authorizing Official and Issuing Authority. Although there is a need to verify identity, the fingerprinting process done up front with new employees verifies they are who they say that are. Requirements in this section seem to be excessive and guarantee that the entire process is slowed down and issuance of ID media to a new employee will be delayed. The requirement of two photo ID's as verification of identity is not practicable when applications are submitted from a distance and interviews are done via telephone and face to face is not done until well into the hiring process. {Physical Security}	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
81	Department of the Treasury	Trung Nguyen	T	Section 2.3, pg. 7	"The Issuing Authority shall photograph the Applicant at the time of issuance and retain a file copy of the image." instructions on the storage of the image is needed. The total number of required copies should be stated to avoid additionat copies being made by Issuing Authority on the premise of just making more in case the first copy is compromised or corrupted. {Privacy}	Some language is necessary to restrict the number of copies of the images or the documents to me make & stored.
82	Department of the Treasury	Trung Nguyen	T	Section 2.3, pg. 7 Section 5.2.1, pg. 41	The applicant must appear in person to the Issuing Authority and the Registration Authority. This is extreme for logical access only. We are a central agency with access internationally. Should this only apply to physical access?	
83		Trung Nguyen		Section 2.3, first paragraph, pg. 7	"The Issuing Authority shall confirm the validity of the PIV request..." What process shall the Issuing Authority use to do this?	
84		Trung Nguyen		Section 2.3, first paragraph, pg. 7	"The Issuing Authority shall be responsible to maintain ... Completed and formally authorized PIV Request." The Registration Authority is also tasked with this in Section 2.2.1. How can there be two completed and signed PIV requests?	
85	Department of the Treasury	Trung Nguyen	G	Section 3.1, pg. 10	Clarify expectation for verifying identity for current employees and contractors. FMS currently has over 3000 employees and contractors. This may create logistical issues for incumbent employees to produce their original birth certificate, passport, etc. prior to issuance of the PIV cards, particularly in cases where original documentation may be lost.	
86	Department of the Treasury	Trung Nguyen	G	Section 3.1, pg. 10	Functional Objects: The objectives stated in this section are to enhance security and privacy. 1. A "one size" fits all standard could result in making it easier to compromise identification media and access controls. 2. In addition this standard appears to limit the agency's ability to determine their security needs based on their assessment of the criticality of the mission, sensitivity of information and sensitivity of the facility.	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
87	Department of the Treasury	Trung Nguyen		Section 3.1, pg. 10	What activities implemented to protect the privacy of a cardholder would constitute due diligence? Additional guidance should clarify the constraints to be observed to avoid over zealous efforts to enable PIV at the risk of encroaching on the card holders rights of privacy.	
88	Department of the Treasury	Trung Nguyen		Section 3.1, pg. 11	To promote the functional objectives of the standard to enable interoperability, an independent interoperability lab and certification authority is needed given the schedule for compliance. This is not a capability that the agencies should duplicate. Interoperability standards and certified products should be published by an independent sources dedicated to validating the quality and reliability of the devices and products required to implement the standard.	
89	Department of the Treasury	Trung Nguyen	T	Section 3.2.1 pg. 11	What is the process for defining position sensitivity at an application? How does this relate to OMB 04-04 or 199?	
90	Department of the Treasury	Trung Nguyen	G	Section 3.2.1, pg. 11	It states that "Federal departments and agencies that issue and use identity credentials will be responsible for: Establishing position sensitivity levels for Applicants". {Policy}	There should be some standard criteria for sensitivity levels.
91	Department of the Treasury	Trung Nguyen		Section 3.2.1, pg. 11	Cooperating with other agencies may require the sharing of source identity information on employees and contractors protected by the Privacy Act across agencies to verify position sensitivity levels. How is the agency responsibility for privacy and data protection to be shared? If an individual makes inquiries or requests information about the information exchanged and its usage, how will such inquires be handled and by whom?	
92	Department of the Treasury	Trung Nguyen	T	Section 3.2.1, pg. 11	PIV-II supports interoperability Government-Wide	FIPS should specify negotiated interoperability between entities instead of inferring mandatory interopoerability government-wide
93	Department of the Treasury	Trung Nguyen	T	Section 3.2.3, pg. 12	Will OMB review and approve operational procedures before going live? Based on what criteria? Will OMB approve or disapprove June 2005 plans?	Clarify
94	Department of the Treasury	Trung Nguyen	T	Section 3.2.3, pg. 12	GSA will assist agencies to operate PIV sub systems? What does this mean?	

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

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
95	Department of the Treasury	Trung Nguyen	G	Section 3.2.3, pg. 12	Will there be procedures/guidance provided for cross-certification of organizations doing applicant authentication? {Policy}	
96	Department of the Treasury	Trung Nguyen	G	Section 3.2.3, pg. 12	Oversight Responsibilities: OMB is responsible for reviewing and approving PIV system budgets and operational procedures. How will funding be provided to agencies to accomplish this. Large organizations (100K plus employees) will require unprogrammed funding in excess of $100M to address this directive. Identifying the funds from existing FY05 and 06 budgets that have already experienced severe cuts will prove difficult if not impossible. In addition to the cost, the amount of time required to refit a large number of highly dispersed government and leased facilities across the country will require a timeline measured in years {3 to 5 likely}. {Physical Security}	Propose OMB issues further guidance on acceptable process for identifying and budgeting unprogrammed costs associated with implementing this directive.
97	Department of the Treasury	Trung Nguyen	T	Section 3.3, pg. 13	Figure 3-1: PIV System Functional Model: In the Fig and in the narrative where the Authorization Data comes from is not evident and neither is what type of data is in the Authorization repository. {Privacy}	Language to ensure that agencies specifically know where this information is to come from and what type of information is needed for the authorization data repository.
98		Trung Nguyen	T	Section 3.3.1, p.14, 1st paragraph	Suggest that the number of ICCs be clearly defined and discrete: "two" rather than "one or more". It would be difficult for the card to interoperate with multiple government agencies if each agency employs cards using varying numbers of chips to hold security/identity data.	
99		Trung Nguyen	T	Section 3.3.2, p.14, 1st paragraph	A complete, discrete set of data should be provided here, rather than examples of data collected. This leaves unnecessary room for interpretation.	
100		Trung Nguyen	T	Section 3.3.2, p.14, 3rd paragraph	The actual security mechanisms need to be clearly defined rather than loosely stated requirements.	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
101	Department of the Treasury	Trung Nguyen	G	Section 3.3.2, pg. 14	Marital status is among the information being collected from applicants during registration. "Information such as full name, address, date of birth, marital status,...are examples of information collected ..." There doesn't seem to be a purpose for the collection of marital status and its use. Example used to pertain to the relevant and necessary data element that can be used for identity proofing. A person's marital status holds no such assurance. {Privacy}	Recommend that we not capture this information. It serves no useful purpose and could change. Change the example data elements to examples that are relevant and necessary of identity proofing.
102	Department of the Treasury	Trung Nguyen	T	Section 3.3.3, pg. 15	The logical resource is typically a location on the network to which the cardholder desires to gain access. Computer workstation is listed as an example. Is the intent to cover Blackberries, pocketpcs and other PDAs?	Introduce the concept of applying OMB 04-04 and 199 here.
103	Department of the Treasury	Trung Nguyen	G	Section 3.4, pg. 15	Card Lifecycle Activities. " Manufactures are not considered part of this lifecycle model." Clarity requested. Manufactures are part of the engineering process within the life cycle? {Policy}	Requires clarity
104	Department of the Treasury	Trung Nguyen	G	Section 4.1.1a, pg. 17	Printed Material. Are ink specifications needed? {Policy}	
105	Department of the Treasury	Trung Nguyen	G	Section 4.1.2 pg. 17	4.1.2 - Optical ink is now required. Will that be an issue for physical security?	
106	Department of the Treasury	Trung Nguyen	T	pg. 17	Does not mention "Ghosting" of photo	Add "Ghosting" of photo
107	Department of the Treasury	Trung Nguyen	G	Section 4.1.3.g, pg. 18	This section states that the PIV card shall not be punched with holes. Some agencies require badges to be worn and visible at all times. Multiple badge clips or badge holders would not be usable with this standard, in turn requiring agencies to remove their current inventory of clips and badge holders.	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
108	Department of the Treasury	Trung Nguyen	G	Section 4.1.4, pg. 19	Topography Requirements: Although mandatory information and requirements for Cards may be a good security practice, each agency has internal requirements for visual authentication for internal controls. The primary purpose of the card is to meet agency needs, all other uses should be secondary. Where the printed information is on a card and how it is formatted around the computer chip, mag stripe or bar code should be left to the agency so that they have the option of focusing on their controls. Differences in cards does allow agencies to immediately differentiate between their employees and visitors which are important internal controls.	
109	Department of the Treasury	Trung Nguyen	T	Section 4.1.4, pg. 19, 1st paragraph	The PIV-II standard SHOULD specify a dual-chip card to ensure future interoperability.	
110	Department of the Treasury	Trung Nguyen	E	Section 4.1.4.1, pg. 19	Add "digital" to the photograph statement.	A digitized pictorial representation...
111	Department of the Treasury	Trung Nguyen	G	Section 4.1.4.1.c, pg. 19	Will there be any provisions for statements or procedures regarding Temporary, Term or Intermittent employees?	Recommend addressing this issue. Will intermittent employees be issued a new card every time they come in?
112	Department of the Treasury	Trung Nguyen	G	Section 4.1.4.2.a, pg. 21	Agency card serial numbers. "Format for the serial number shall be left to the agencies discretion" {Policy}	No standard format will lead to information sharing/ database problems between agencies.
113	Department of the Treasury	Trung Nguyen	G	Section 4.1.4.4.d, pg. 20	Place a reference for determining the standards for this designation (Emergency Responder).	This designation has the potential to be abused and the standard reference needs to be clearly stated.
114	Department of the Treasury	Trung Nguyen	E	Section 4.1.4.4.f, pg. 20	Edit text as follows:	...may be printed on the bottom back...
115	Department of the Treasury	Trung Nguyen	T	Section 4.1.5, pg. 23	Two bio fingerprints AND bio facial image are significant overkill for the risk levels of many applications and physical locations. What is the justification for this requirement?	
116	Department of the Treasury	Trung Nguyen	T	Section 4.1.5.1, pg. 23, 1st bulleted list	The standard should specify exactly how many key pairs and corresponding certificates should be stored and accessed on the card. Suggest exactly three - one for encryption, one for authentication (local and otherwise) and one for digital signature.	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
117	Department of the Treasury	Trung Nguyen	T	Section 4.1.5.1, pg. 23, 2nd bulleted list	An exact set of keys/certificates should be defined, not leaving it up to each agency. This makes interoperability difficult.	
118	Department of the Treasury	Trung Nguyen	T	Section 4.1.5.1, pg. 23		Make biometric facial optional not mandatory. Cite fingerprint as preference and other biometric as option.
119	Department of the Treasury	Trung Nguyen	E	Section 4.1.5.2, pg. 21	Edit text: priori.	Should be: prior
120	Department of the Treasury	Trung Nguyen	G	Section 4.1.6.1, pg. 24	Guidance should be specific in regards to the limiting number of activation attempts. {Policy}	
121	Department of the Treasury	Trung Nguyen	T	Section 4.1.6.1, pg. 24, 2nd paragraph	Standard should specify PIN construction - # of digits, no alpha chars, etc.	
122	Department of the Treasury	Trung Nguyen	G	Section 4.1.6.2, pg. 24	Paragraph one refers to a Global Platform challenge response. It further states card management keys shall be specific to each PIV card. If this is a reference to, or endorsement of, key diversification of a KMC value please provide reference to the acceptable use of key diversification. If diversification is not acceptable, than the volume of symmetric keys to manage may be impractical.	
123	Department of the Treasury	Trung Nguyen	T	Section 4.2.1, pg. 25	Standard should provide a table listing the entire CHUID contents and data elements, rather than pieces in separate tables. It is difficult to conceive of what the CHUID actually looks like to the system when it is presented in such abstraction.	
124	Department of the Treasury	Trung Nguyen	T	Section 4.2.1, pg. 25	How does this expiration date compare with digital certificate expiries, or the date printed on the card? Is there an order of precedence or are these envisioned to be processed/handled independently?	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
125	Department of the Treasury	Trung Nguyen	T	Section 4.2.2, pg. 26, last paragraph	What about PKIs that are currently cross-certified with the Federal Bridge? As stated elsewhere, Certification Authorities belonging to such PKIs are valid for PIV purposes, so they should be valid here.	
126	Department of the Treasury	Trung Nguyen	E	Figure 4-2, pg. 20	Add Non-Military to Figure Title.	UNIVERSAL LANGUAGE - Non-Military
127	Department of the Treasury	Trung Nguyen	G	Section 4.3, pg. 27	Cryptographic Specifications: If cryptographic operations are performed using the PIV card stored with one of the keys mention, mandatory compliance with National Security Telecommunications and Information Systems (NSTISS) No. 4001 "CONTROLLED CRYPTOGRAPHIC ITEMS" could be an issue. {Physical Security}	Propose the standard address special handling of cryptographic key material if such requirements are anticipated. If stringent handling requirements exists, standard should direct to appropriate reference to properly address incidents as they may arise (e.g. lost cards, compromised materials, etc....)
128	Department of the Treasury	Trung Nguyen	G	Section 4.2.2, pgs. 27-29	Since PKI signing keys will be stored on the PIV card, we should use the same card to store PKI encryption keys.	Add PKI encryption key to list of optional keys
129	Department of the Treasury	Trung Nguyen	T	Section 4.3, pg. 27, 1st paragraph	At least two certificates should be specified. Exactly three are suggested - one for encryption, one for authentication (local and otherwise) and one for digital signature.	
130	Department of the Treasury	Trung Nguyen	T	Section 4.3, pg. 27, 4th paragraph	AES should either be required or not. Leaving room for interpretation makes it more difficult for the card to be interoperable.	
131	Department of the Treasury	Trung Nguyen	T	Section 4.3, pg. 27, 4th paragraph	A specific certificate should be specified for contactless interfaces utilizing asymmetric keys.	
132	Department of the Treasury	Trung Nguyen	T	Section 4.3, pg. 27, bulleted list	Specific certificates should be required, without options, for maximum interoperability. Suggest an encryption, authentication and digital signature certificate.	
133	Department of the Treasury	Trung Nguyen	T	Section 4.3, pg. 29, 4th paragraph	Not specifying key management protocols as part of PIV-II will severely limit interoperability, both in the physical and logical realm.	

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

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
134	Department of the Treasury	Trung Nguyen	T	Section 4.3, pg. 29, last paragraph	Standard should explicitly specify whether or not trust anchor certificates will be required on the card, rather than making it optional. There are good reasons for inclusion of trust anchor certificates on the card itself (mainly, secure and trusted distribution channel for this data). Also, the number of trust anchor certificates that may be allowed is important since logical memory is limited on the chip.	
135	Department of the Treasury	Trung Nguyen	T	Section 4.4 pg 30	How, where and for how long am I storing 10 bio fingerprints?	
136	Department of the Treasury	Trung Nguyen	G	Section 4.4, pg. 30	What do they mean by one-to-many fingerprint recognition during the application process? Does this mean we need to maintain a database of everyone's fingerprints to ensure no duplicate requests? I think this was something that was brought up during our last comments.	
137	Department of the Treasury	Trung Nguyen	T	Section 4.4, pg. 30	Pixel standards for photos require mega resolution cameras. No industry agreement on what constitutes center of the eye or interocular distance.	
138	Department of the Treasury	Trung Nguyen	T	Section 4.4, pg. 30	Biometrics -- this section prescribes storage of fingerprint image on the card instead of as a template. This presents both privacy and technology problems. On the privacy side, use of image versus template raises a number of concerns form privacy advocates, as an image may be easier for nefarious interests to abuse. On the technology side, there are serious concerns as to whether there is enough space on a smart card to carry two finger index images. In addition, the increased processing time associated with a match of a finger image stored on a smart card vs. a match of a template can lead to degradation of overall system performance -- translating to longer lines and delays in system functionality in real-world systems.	Adopt a standard template for fingerprint storage as part of PIV.

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
139	Department of the Treasury	Trung Nguyen	T	Section 4.4, pg. 30	This section prescribes very strict limitations on how contact and contactless cards may be used or not used, as well as how biometrics may be used in concert with them. These limitations are overly restrictive, fail to anticipate both future card platforms (such as combi cards) and innovations in chip and biometric technology, and would unnecessarily constrain agencies in their applications of card and biometric technology. For example, agencies would be precluded from doing physical access control with a contactless chip and biometric.	Permit biometrics to be used on both contact and contactless cards. Permit contactless PKI transactions if they can be done in a manner consistent with FIPS 140 validation. Eliminate any mandates which require contact chip or contactless chips to be used for only certain purposes, and instead allow either technology to be used for any purpose, so long as it can be done in a way that is compliant with FIPS 140.
140	Department of the Treasury	Trung Nguyen	G	Section 4.4.1, pg. 30	Biometric Specifications: Is the ten fingerprints requested for support of law enforcement check during the application process either "slap" or "rolled" as mention in section 4.4.1 PIV Registration (Biometric Enrollment) and Issuance? {Physical Security}	Propose the standard specify capture process for fingerprints.
141	Department of the Treasury	Trung Nguyen	T	Section 4.4.6, pg. 37	What and whose key should be used to protect this biometric data?	
142	Department of the Treasury	Trung Nguyen	T	Section 4.5.3, pg. 39	Using this PIN as activation data in both physical and logical instances may be difficult - typically physical access control systems utilize a 4-digit PIN for convenience and moving people faster; whereas logical systems use a strong password. Not having the exact PIN construction (which is needed in this standard) makes it difficult to assess how this will be implemented, but the WHAT and HOW should be specified.	
143	Department of the Treasury	Trung Nguyen	G	Section 4.5.2, pg. 39	In this section it states "physical access control systems where the readers are not connected to general purpose desktop computing systems, the reader-to-host system interface is not specified in this standard. This is necessary in order to allow retrofitting of PIV readers into existing physical access control systems that use a variety of nonstandard card reader communications interfaces". Although the interface is not specified in this standard it does reference the ISO/IEC 14443 standard which specifies reader types and frequencies which in turn limits the retrofitting of PIV readers.	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
144	Department of the Treasury	Trung Nguyen	T	Section 4.5.2, pg. 39	ISO 14443 is insufficient standard for RFID transmissions. Industry uses hundreds of standards. Interoperability issues.	
145	Department of the Treasury	Trung Nguyen	T	Section 5.1.1 pg. 40	Mandatory elements of the registration database should be listed. Does this contain the entire background check or just date and status? Does this contain the IA data too?	List mandatory data elements
146	Department of the Treasury	Trung Nguyen	T	Section 5.1.1, pg. 40	There should at least be a reference to the Common Policy for access control to repositories storing PIV data at rest.	
147	Department of the Treasury	Trung Nguyen	E/T	Section 5.1.2, pg. 40, 3rd paragraph	"CA certificates needed to build a path to the Federal Bridge CA." is poorly worded. Assuming that "Federal Bridge CA cross-certified certificate" is meant, there should also be a provision included for path processing to the Common Policy Root - as would be the case in most path validation situations.	
148	Department of the Treasury	Trung Nguyen	E	Section 5.2.1, pg. 40	This section belongs with PIV-I	
149	Department of the Treasury	Trung Nguyen	E	Section 5.2.1, pg. 41	Second and third bullets are one sentence.	
150	Department of the Treasury	Trung Nguyen	T	Section 5.2.1.1, pg. 40	Has a legal opinion been obtained from INS on references pertaining to the I-9? The Immigration Act of 1990 added a requirement that employers could not discriminate against employees by requesting more or different documents. Therefore the statement in this paragraph that at least one of the documents shall be a valid State or Federal Government issued picture ID may be illegal. Also the sole intent of the I-9 is for employment verification to ensure that employers are not hiring illegal immigrants. It was not meant to be a source for verifying identify. Recommend staying away from any references to the I-9, but rather go with a listing of documents that are appropriate for verifying identity. Rationale is that the I-9 is very restrictive as to the uses and the fact that agencies cannot dictate to an applicant the documents that they should provide.	Develop a clear and concise policy for validating identity which is separate and apart from the employment verification process as required by the Immigration Reform Act of 1986 (for the I-9 process.) Recommend criteria contains two source documents, one of which would be government issued picture ID media.
151	Department of the Treasury	Trung Nguyen	E	Section 5.2.1.1, pg. 41	Second bullet: Remove the third bullet and bring that sentence up to be a part of the second bullet. {Policy}	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
152	Department of the Treasury	Trung Nguyen	G	Section 5.2.1.1, pg. 41	Table 5-1: The Form I-9 is not intended to collect information for a background investigation. It does not contain the necessary information needed for a background investigation nor does it contain the Authorizations for Release of Information. The I-9 should not be used for personnel security background investigation purposes. IRS uses the SF-85P for all position risk sensitivity levels on contractors; the SF85 for low risk employees, the SF85P for moderate and high risk employees; and the SF-86 for national security. {Policy}	Recommend change to show use of the Form SF-85, Questionnaire for Non-sensitive Positions or equivalent for Level 1 - low risk; SF-85P for level 2 and 3 - moderate and high; and SF-86 for level 4 - Critical
153	Department of the Treasury	Trung Nguyen	E	Section 5.2.1.2, pg. 42	Change expect to except.	
154	Department of the Treasury	Trung Nguyen	E	Section 5.2.2, pg. 42	This section belongs with PIV-I	
155	Department of the Treasury	Trung Nguyen	T	Section 5.2.2, pg. 43	The Issuing and Registration Authority should be only optionally separated into two roles - not mandatory. Also, is the IA being referenced here a person or thing? It is assumed that it's a thing since it's digitally signing something, but as other roles are inherited by people, this should be clearly defined.	
156	Department of the Treasury	Trung Nguyen	T	Section 5.2.2, pg. 43	Much more detail is needed here - what is the strength of the "one time authenticator" value? How is it generated, what algorithms are used, how is it transported, how is the OTP function upheld, etc. If the user is required to generate answers to personal questions in the event they forget their PIN, when/how is this done? Nowhere in the document is this stated - do we assume that it's not part of PIV for security reasons? If so, people should be aware of the administrative impact as people forget their PINs and require resets.	
157	Department of the Treasury	Trung Nguyen	T	Section 5.2.3, pg. 43	There should be a statement of waiver for organizations with CAs that have cross-certified with the Federal Bridge CA. Those CA certificates should be allowed in PIV. Any subsequent references to the Common Policy should also reference the CPs of cross-certified CAs. It this statement is made elsewhere in the document, it should also be noted here or at least a reference provided to the appropriate section.	

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
158	Department of the Treasury	Trung Nguyen	T	Section 5.2.3.3, pg. 45	It should be clarified that CAs should make CRLs *publicly available* every 18 hours, rather than issue them. Additionally, what about ARLs for issuer revocation information? This document does not specify issuer certificate revocation information.	
159	Department of the Treasury	Trung Nguyen	T	Section 5.2.3.4, pg. 45	ALL certificates should be made available using LDAP. Not sure why the statement was made that authentication certificates should not be placed there. This should be mandatory, not left to agencies.	
160	Department of the Treasury	Trung Nguyen	T	Section 5.2.3.5, pg. 45	OCSP should be optional, not required. Also, which version of OCSP, and what about SCVP?	
161	Department of the Treasury	Trung Nguyen	T	Section 5.2.3.6, pg. 46	Having this single reference to these organizations is not sufficient - the references should be made whenever the Common Policy and its associated infrastructure is referenced.	
162	Department of the Treasury	Trung Nguyen	G/E	Section 5.2.4, pg. 46	A flow chart would be helpful to explain each of the card lifecycle management functions to visually depict where the user and the related Authorities interact.	
163	Department of the Treasury	Trung Nguyen	T	Section 5.2.4.1, pg. 46, 1st paragraph	Isn't this the responsibility of the RA, rather than the IA?	
164	Department of the Treasury	Trung Nguyen	T	Section 5.2.4.1, pg. 46, 3rd paragraph	What are the procedures for safe/secure disposal of card data?	
165	Department of the Treasury	Trung Nguyen	T	Section 5.2.4.2, pg. 46, 2nd paragraph	It is unwise to suggest that cards should be reissued upon PIN lockouts - there should be an alternative stated. Reissuing cards every time a PIN is forgotten will, in practice, be too operationally intense to be practical in 99% of cases.	
166	Department of the Treasury	Trung Nguyen	T	Section 5.2.4.2, pg. 47	What is the PIV Certificate Issuer? Is this the Issuing Authority? This is the first reference in the document. Also, this should reference the Common Policy and FBCA Policy for procedures.	
167	Department of the Treasury	Trung Nguyen	T	Section 5.2.4.2, pg. 47	Since OCSP should be optional, only CRL updates should be required. Also, which version of OCSP, and what about SCVP?	

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

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
168	Department of the Treasury	Trung Nguyen	T	Section 5.2.4.2, pg. 47	This one-hour emergency provision is the first reference in the document. This should be stated everywhere there is an 18-hour reference, as it appears in several other areas.	
169	Department of the Treasury	Trung Nguyen	G	Section 5.2.4, pg. 46	This section dealing with the renewal and re-issuance of the PIV conflicts with Section 2.2.2. This conflict creates two different standards in the above aspects.	
170	Department of the Treasury	Trung Nguyen	T	Section 5.2.5, pg. 47	There are other cases warranting PIV termination, such as when the PIV cardholder has been found in violation of their signed agreement; committs acts against the government; etc.	
171	Department of the Treasury	Trung Nguyen	T	Section 5.2.5, pg. 48	Since OCSP should be optional, only CRL updates should be required. Also, which version of OCSP, and what about SCVP?	
172	Department of the Treasury	Trung Nguyen	G	Section 5.2.5, pg. 47	5.2.5 Since cards are issued by a specific Issuing Authority termination should be at that level and not "federal service". To the reader it implies that cards are not terminated when a user transfers from one federal agency to another. Was this the intention?	
173	Department of the Treasury	Trung Nguyen	G	Section 5.2.5, pg. 48	Destroying Card	Need clear guidance and instructions on the methods for destroying these cards and what to do with the remains.
174	Department of the Treasury	Trung Nguyen	G	Section 5.5.1, pg. 42	1st paragraph under the tables: It requires that a successful completion of a background investigation is required before issuance of a PIV. In IRS, we approve employees for access based on successful completion of a fingerprint screening before EOD and contractors must pass an interim determination of a fingerprint and tax check for unescorted access. Completion of a background investigation before issuance of a PIV would impact successful business measures. {Policy}	Allow agencies to implement interim procedures while background investigation is being completed.
175	Department of the Treasury	Trung Nguyen	E/G	Section 6	This should be an appendix if it is informational only. It is not appropriate in the body of a standards document. Suggestion that it be included as part of Annex B.	
176	Department of the Treasury	Trung Nguyen		Section 6.1.1, pg. 50	Agency name or department is an optional attribute for PIV card.	Agency name should be mandatory attribute for PIV card.
177	Department of the Treasury	Trung Nguyen	T	Section 6.1.2, pg. 51	This document is unclear on the purpose of the CUID, as this is the first reference in the document and it is not explained. The acroynms section provides little detail or explanation. Where the difference between the FASC-N and the CUID explained?	

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

Cmt #	Org.	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc. and Page Nbr	Comment (Include rationale for comment)	Proposed Change
178	Department of the Treasury	Trung Nguyen	T	Section 6.1.3, pg. 52	This prescribes a very specific means of using PIV Biometric credentials that is very cumbersome and not reasonably applicable to using a biometric for logical access applications. If an agency wanted to use the biometric stored on the card to access a certificate or network resource, the application would involve both PIN validation as well as extensive interaction with the CHUID. Putting such limitations on an agency application of biometric technology goes far beyond the scope of what was envisioned in HSPD-12 and would severely limit the ways in which the PIV card and the biometrics it contains would be able to be used in a variety of agency applications.	Lift these onerous restrictions out of the FIPS 201 specification. Do not require PIN entry as part of an agency biometric validation application.
179	Department of the Treasury	Trung Nguyen	T	pg. 49	Contactless use of PIN & Biometric not supported	Makes 14443 useless for physical access
180	Department of the Treasury	Trung Nguyen		Appendix A	This entire section treats accreditation as a hardware issue. Use of secure hardware and software modules by unreliable operators does nothing to ensure the chain of trust and level of confidence required for cross-agency interoperability. While SP 800-37 includes personnel in its definition of Information Resources, FIPS 201 must address operator accreditation, otherwise, Agencies will continue to refuse to accept credentials issued by others.	
181	Department of the Treasury	Trung Nguyen	T	Section B.2, pg. 65	This incorporates by reference OMB's E-Authentication guidance, however it provides no detail as to how PIV relates to this new and very important government mandate. At a minimum, somewhere it should be noted that PIV identities are required for logical access to all systems evaluated to assurance level 4.	
182	Department of the Treasury	Trung Nguyen	G	Sections 3 & 6, pg. iv-v; Sections 1.1 & 1.2, pg. 1	This first reference states, "This standard does not specify access control policies for agencies." However, in this section and throughout this FIPS, there are various references making vague references to access control to information systems. If there will be specific criteria established elsewhere, or if each agency will be left up to their own means, it needs to be stated somewhere. {Operational Assurance}	Establish specific reference for agencies to refer to for access control to information systems.