Department of Energy
Comments on
Personal Identity Verification for Federal
Employees and Contractors
And
Integrated Circuit Card for Personal Identity Verification

December 23, 2004

I. Introduction

Thank you for this opportunity to comment on this guidance. If you have any questions, please contact Bruce Brody, Associate CIO for Cyber Security, at (202) 586-7865.

General Comments and Observations for FIPS 201

General Comments:

(1) Certain technologies identified in FIPS 201 may have significant challenges in an enterprise implementation. We recommend that FIPS 201 be altered to incorporate trigger mechanisms that would activate certain technologies when government has been able to valid the feasibility of these technologies. DOE believes that this should be predicated on an operational demonstration, and not merely an academic lab test. DOE would recommend that FIPS 201 consider language requiring an Office of Management and Budget (OMB) memorandum to all heads of agencies triggering these technologies when all appropriate questions have received proper consideration and the government understands the impacts more fully.

(2) DOE has concerns that government is adopting an approach that does not have an existing reference implementation. When we evaluate the security landscape, we do not see an example that would indicate that the FIPS 201 has ever been achieved in an enterprise operational environment previously. We see a number of cases of failed implementation for aspects of FIPS 201. Minimally, DOE believes that OMB should establish an appropriate forum to establish and share reference implementation guidance to avoid duplicate efforts across government that will raises costs, and adversely impact on interoperability.

(3) DOE currently has a balance of seven contractors for every eight total (employees and contractor) staff members, acting under separate contractual agreements that have significantly different structures. DOE has not been able to fully assess the impact and requirements to modify existing contracts, which may impact on our ability to follow the timelines under HPSD-12 if FIPS

201 is implemented.

(4) DOE believes that the intent of FIPS 201, as drafted in the original format and in the IAB format mandates biometrics that will create significant cost and privacy issues. DOE does not yet see a compelling business case, especially for the requirement to establish a biometric repository, which may create conflict with our labor unions. DOE also has concerns that federal standards have not been adopted, and are not expected to be adopted prior to February 25, 2005 when FIPS 201 will be officially published.

(5) DOE requests that FIPS 201 be modified to provide clear language related to the application of A-76 contractor services, and what portions of FIPS 201 are "inherently governmental." In particular, the roles that are identified in FIPS 201 should be addressed.

(6) DOE believes that FIPS 201 will require the creation of new data systems; that these data systems will contain privacy act information and that each federal agency will be require to evaluate compliance under the legal mandates associated with "system or record" statutes. As such, DOE asks NIST and OMB to provide guidance and direction in this area.

(7) DOE believes that aspects and certain technologies, as represented by vendor products in the marketplace, will not be Section 508 compliant. DOE asks NIST to consider this in FIPS 201.

(8) HPSD-12 requires NIST to identify graduated criteria to address implementation. DOE does not believe that FIPS 201 in the original version of in the IAB version properly addresses the intent of graduated criteria. DOE would like to see further consideration given to this section, which should not merely identify technical alternatives.

(9) DOE believes that the intent of FIPS 201, as drafted in both the original and IAB format cannot be achieved in a cost effective manner without significant attention to interoperability across government agencies. It is not prudent to require a common solution for government, but leave architecture, implementation and management up to each individual agency. Further, DOE understands that no new funding will be provided to address FIPS 201 requirements. -

(10) DOE recommends that OMB identify a federal resource to coordinate a common interoperable architecture, implementation details and management of common system(s) required in FIPS 201 in a cost effective manner. A federal budget should be established and funded to support this activity.

(11) While DOE supports the mandates of HSPD-12, we believe that the implementation details contained in FIPS 201 and the pending review of NIST

Special Publication 800-73 should balance the benefits, the state of technology, and the risks to be mitigated to protect what will turn out to be an expensive investment by the government.

(12) Implementation of the PIV system will require major human capital (employee resources) and financial capital (financial resources). Many federal agencies are currently ill equipped and lack the resources necessary to handle the requirements and the implementation of the PIV system given the short time frame of October 2005. This effective date is unrealistic and will result in standards not being met. A graduated approach would be an effective way to handle the implementation. It would give the necessary flexibility for each federal agency.

(13) This draft document lacks guidelines on the types of sites that should be card-key accessible. It is assumed that some type of key system is in place, but again, there is no information on what type of site should be guarded, or any indication that this decision should be left to each site manager. -

(14) In general, this is a well designed document and it touches all the right areas. However, the initial issue will be the position sensitivity requirement, and the corresponding background checks. More specifically, even if the processes were aligned and the requirements implemented "top-down," the big question will be what to do about existing credential holders. The position sensitivity requirement implies that all personnel will have to be reclassified according to sensitivity and also be vetted out by potentially new background checks. What would the unions and EEO impacts be? Concerned that this could be a potential legal "nightmare."

(15) The technical specifications within the draft document point toward complex and expensive PIV systems in the future that meet the FIPS 201 requirements. This could take years and be very expensive to DOE and other Federal agencies. As to the biometrics aspects, believe it would be necessary for someone who has direct experience with these kinds of systems' expected false-positives-and-negatives to be able to judge whether the proposed parameters are reasonable.

(16) HSPD-12 and this standard (FIPS 201) need to take into account other Federal requirements that require organizations to operate on a risk and vulnerability management based approach. To simply require that all federal sites implement the program required by this standard does not allow for a true risk based determination of the need. Suggest using a graduated approach that allows organizations to make a risk based decision to follow or not follow the FIPS 201 requirements or to adjust the level to which they follow this standard.

General Observations:

(1) This is a case where establishing a publicly-available standard across federal agencies for access control can actually make security weaker. The current paradigm of disparate control mechanisms and ID forms, while more onerous and harder to unify and manage, makes it harder for attackers. Attackers have to exploit different system types and spoof different ID types, thus increasing their chance of being caught. A single more unified system, based on common design, can ease the attacker's job. In addition, a common system framework can foster a sense of trust in those performing verification processes. If a credential presenter provides false credentials, a verifier might too easily chalk up a problem to "a system glitch" because after all, the person is providing "valid" credentials and it "should work." The mentality centers around "if it looks, walks and acts like a duck, it MUST be a duck." This is a big reason why it is easy to commit white collar crime, because control & verification systems at large institutions are abstracted from the front-line "worker bees," making it easy to exploit them.

(2) This draft document does not define the necessary requirements for contactless PIV cards that are an important emerging technology which require a more detailed discussion for secure use than is provided in this document. By not properly addressing the requirements for contactless PIV cards, NIST does Federal agencies a disservice and prevents them from implementing this modern technology. We believe that NIST has two options: either include references to contactless PIV cards in this standard or remove all references to contactless PIV cares from this standard and label this standard as referring to only contact PIV cards. Then NIST can prepare an additional standard with sections that specify the proper, secure use of contactless PIV cards.

(3) From a DOE security standpoint there are a variety of issues that are either not addressed or not fully addressed in HSPD-12 and the background information provided by NIST. A clear issue is the reference to an identification card, "forms of identification", we have been interpreting this to mean the equivalent of our DOE standard badge. That is a badge worn in clear view above the waist, often around the neck on some sort of lanyard. However this may be because of the package prepared by NIST which models a security badge type form of identification. It is unclear the intent of HSPD-12 and could be argued that the badge would appear to function like a driver's license unlike the standard DOE issued badge. If this were the case a number of our concerns as described below would be eliminated.

   a. An obvious issue is the lack of funding data. The initial cost of the badges will be dwarfed by the cost of the access control systems that would require modification to accommodate the new standard. However, even for the cost of a badge alone there is considerable cost differences based on the type of card or badge selected, (magnetic

stripe cards less $1 each, smart cards more than $6 each). The department may be unusually impacted in the access control area due to the large number of different security areas of varying levels in the Department. We have not only the access controls at our purely administrative offices such as Germantown and Forestall but also the more stringent requirements at our nuclear facilities. Some sites have gone through major systems upgrades recently and absent a very large infusion of cash will not be able to easily fund the level of cost associated with the required modifications.

b. If the intent is for these "form of identification" to replace rather than supplement the DOE standard badge, then this department's use of security badges for visual identification of employees, contractors and their security clearances would be severely impacted. In addition we require foreign visitors to be clearly identified with a distinctive red badge. We also issue very large numbers of visitor badges for individuals outside the government. How these special situations would be addressed with the adoption of the standard federal government identification is not known. The DOE security requirements may not be able to be accommodated through HSPD-12. If this is the case the requirement for the adoption of the new badge could lead to DOE having to maintain a dual badge system. The two would be the new national badge and a badge similar in design and purpose to the current DOE standard badge. Another possibility would be to carry the new card as a form of identification like a driver's license but to have the standard DOE badge as the routine form of identification within the DOE work complex.

(4) DOE Security Police Officers still have to be able to see and recognize the distinctive DOE standard badge, sometimes at a distance. While more and more automated access controls are being utilized officers still must be able to easily recognize the badge each person is wearing as a means of quickly identifying if individuals are authorized access to a site, a facility or a particular area. In addition, in classified meetings attendees have to have a simple means of determining if those present are cleared for the level of the meeting. The current standard color coded and clearance denoted badges serve the above purposes. They also have built in the ability to store a variety of data that allows security systems to read the badges. The proposal in HSPD-12 would not allow easy recognition of DOE employees and contractors or their clearance level. Mere possession of the proposed badge would not make clear, except at very close quarters, a DOE employee from a USDA employee or identify a cleared from uncleared person. While the smart technology planned for the cards would or could contain this level of information there are circumstances where the type of reader required would simply not be available.

(5) The requirement for government computer systems to be accessible through the use of the new badge is also somewhat confusing. The confusion stems from what appears to be an attempt to strengthen the security of government computer systems by requiring the insertion of the card into the system as a first step in authentication. It is not clear how this is better than the current password and pin system. In addition what systems are being secured through this additional requirement? National security systems are exempt from the requirement so only those operating at an unclassified level would be covered by the new requirement so why add this cost of modifying all the computers to have a card reader. It would appear to be a heavy cost to basically protect against waste fraud and abuse of government system if it does not apply to our classified systems.

(6) An additional concern noted in the NIST package, (through not in HSPD-12 itself) is the very broad brush approach to issuing the cards not only to Federal employees and contractors but to all sorts of others to include state and local personnel, university employees and the news media. Having a one size fits all approach to badges or forms of identification are troublesome from a security standpoint. Even more troubling is the intent included under future activity to some how coordinate with foreign government employees for mutual access.

General Comments and Observations for NIST SP 800-73

(1) Find the document to be well organized and easy to follow, however, there are serious problems with references made to other sections within the document. Please see the "General" comment for NIST SP 800-73, under Section II, Comments.

(2) It appears that the document is a programming API "cookbook", and the "flip" side is that it provides hackers a nice reverse engineering tool to exploit systems that are based on the standard (FIPS 201).

II. Comments

Section Reference	Comment
Comments on FIPS 201	
General	All fourth-level sub-titles (e.g., 4.1.5.2 File Structure) need to have a space between the sub-title and the first paragraph. Without a space between the fourth-level sub-title and its first paragraph, it is very easy to consider this paragraph to be an additional paragraph of the third-level sub-title (e.g., paragraph 4 of Section 4.1.5).
Abstract: Section 3	The "Explanation" (Section 3) re-states the HSPD incorrectly and in essence makes it a requirement that Federal agencies be using the standard for identification (Cards) that are issued to employees no later than October (8 Months after the issuance of the standard) of 2005. The HSPD says "to the extent practicable". This language needs to stay in the standard explanation and throughout the standard. The magnitude of this change and the cost-to-accomplish makes it difficult to meet the established time-frame. Page iv, Section 3, paragraph 3, sentence 2. The sentence reads: "PIV-1, describes the minimum requirements for a Federal personal identification system…but does not address the interoperability of PIV cards and systems among agencies." Suggest revising the sentence to delete: "but… among agencies". Since the reader does not have the text of HSPD-12 before him/her, the discussion on the standard should retain the "affirmative approach" of the Abstract that discusses primarily what the standard actually includes. The discussion that states what the standard does not include seems to be confusing. Top of page v, Section 3, paragraph 3, last sentence. "The standard does not specify access control policies for agencies." Suggest deleting this sentence for the same reason as discussed in the previous comment.
Abstract: Section 9	Bottom of page v and top of page vi, Section 9. Attempting to effectively evaluate every position in an agency for security level, and to provide appropriate checks (meeting the criteria provided in PIV-I) is likely to be unachievable for many organizations. Some Federal organizations have not even come up to speed on their information security levels since the implementation of Critical Infrastructure Information (CII). This time table (October 2005) is too aggressive. Suggest that a more gradual schedule be assigned that will allow Federal organizations to plan and budget for the necessary work.
Abstract:	Page vi, Section 10, paragraph 4. Paragraph 4 states that the

Section Reference	Comment
Section 10	standard be reviewed every 5 years. A 5-year cycle in the review of standards may not be a rapid enough schedule to allow adaptation to new threats or new security issues.
Abstract: Section 11	Page vi, Section 11. Though the law does not allow for waivers, there needs to be accommodation for the reality of budget, workload, and other impacts. The standard must reflect the technological capability of sites and should allow flexibility dependant upon the sites' sensitivity level and the technical capabilities. Rather than a waiver, a segmented approach should provide for a variance that allows sites flexibility.
Introduction: Section 1	Page 1, paragraph 3, last sentence. The text reads: "However, this standard does not specify physical and logical access control mechanisms." Suggest deleting this sentence for the same reason as explained in second comment for "Abstract: Section 3." Following the first paragraph on page 2. Suggest inserting a new subtitle: "1.3 Target Audience." Add related text that discusses the intended audience (e.g., Physical or Cyber Security program managers, project managers and System Administrators) to make the text easy to follow. The original subtitle "1.3 Document Organization" can become new subtitle "1.4 Document Organization."
Introduction: Section 1.3	Page 2, paragraph 1 of Section 1.3, sentence 2. The sentence reads: "The first part (PIV-I)…..including the personal identity proofing process, but does not address the interoperability of PIV cards and systems among agencies." Suggest deleting "but does not address…agencies." This part of the sentence is not needed. Page 2, paragraph 2 of Section 1.3, sentence 4. The text reads: "Section 2 of the standard is normative…." Provide a definition for "normative" in this context particularly as the term is repeated later in the next sentence.
PART 1:PIV-I Section 2	Page 4, paragraph 1. This introductory paragraph is misleading and confusing. Suggest removing the phrase "and security objectives" from sentence 2. It appears that Section 2 discusses "security controls," and does not discuss "security objectives." A discussion of "security objectives" could be added to Section 2. Also, suggest removing the phrase "but does not address interoperability of PIV cards and systems among agencies or compel the use of a single, universal credential," because mentioning items NOT covered by the standard can be confusing.
PART 1:PIV-I Section 2.1	Page 4, paragraph 2 of Section 2.1, sentence 1. The text reads: "In PIV-II these identity proofing and issuance requirements are maintained, and a common Government-wide, interoperable PIV

Section Reference	Comment
	card is required." Does this mean that the card will be common in appearance or in operation? If in appearance this may not be a problem, however, we have already experienced damage problems when attempting to use the same card in similar systems across DOE. When staff from our Portland, Oregon office travel to HQ and have their card programmed to grant access to DOE HQ, it damages the information on the card. With the variety of systems already in existence, and the varying need for access control, it is not necessarily a good idea that technologically speaking, an attempt be made to make the cards "interoperable" unless the term is defined to mean that they "could" be made to function across systems, but do not have to, and can remain in their organizationally programmed native mode. Page 4, paragraph 2 of Section 2.1, sentence 2. Certification and Accreditation is not "established" or discussed within PIV-I, however, Annex A of this document provides a detailed discussion of PIV Validation, Certification and Accreditation. Need a reference to Annex A.
PART 1:PIV-I Section 2.2	Page 4, paragraph 1 of Section 2.2, sentence 2. It is stated that, "It should be noted that one individual shall not assume more than one role in this process." It may not be possible to implement this if there is a lack of resources. For example in the case at DOE BPA, the PIV Authorizing Official and the PIV Issuing Authority could be the same office or the same employee.
PART 1:PIV-I Section 2.2.1	Pages 5 and 6, paragraphs 1-5 of Section 2.2.1 (that discuss Identity Proofing and Registration) and Tables 2-1 and 2-2. From a work logistics perspective it could be problematic, to require that all agencies and units use the Federal background clearance process. The turnaround time to get back a NACI or DOE FACTS review can go beyond the time frame within which a contractor may be needed to perform a job. It can delay high impact and high dollar projects. It would be better to define the level of check, and allow the organizations to provide that level through whatever means they choose. Page 5, second paragraph of Section 2.2.1, sentence 3. Text reads: "At least, one of the documents shall be a valid State or Federal Government-issued picture ID." A picture ID whether state or federally issued may not be valid. While it should be one of the forms of identification required, it should not be a deciding factor that is weighted higher than, for example, a fingerprint report. Top of page 6, Table 2-2. "Level 3" and "Level 4" are exactly the

Section Reference	Comment
	same. Suggest revising the table by removing the extra row. In the "Position Sensitivity Level" column for row three, add: "3 and 4."
PART 1:PIV-I Section 2.2.3	Page 7, paragraph 1 of Section 2.2.3. Agree with this paragraph, however, it should be pointed out that it does not address IT access. Is it the intent of the standard that access to cyber assets and information be prohibited or limited during the interim time-frame? This may not be the case in many organizations today and could cause problems in filling positions that are critical within a reasonable time frame.
PART 2: PIV-II General	This section appears to indicate a common system across all agencies. Who will maintain this system, and how will it be kept up to date? We know from our own DOE regional systems how difficult the "care and feeding" of this type of system can be. Implications are either a central government-wide office or the addition of staff to all locations to perform maintenance. There needs to be some degree of assurance for the access control portion of the system. There is no set-aside element (bulleted item) in Oversight Responsibilities (Section 3.2.3) or Functional Components (Section 3.3). The "Access Control Subsystem" is mentioned within Section 3.3, Functional Components as a sub-system that is not covered in detail within this standard. This is also an issue on pages 22 (Section 4.1.4) and 23 (Section 4.1.5) of this document that mention and briefly discuss the access control components, for the purposes of this standard. Suggest if feasible, including a detailed discussion of the "Access Control Subsystem" and/or assurance for this sub-system within the scope of this standard.
PART 2: PIV-II Section 3.1	Page 10, paragraph 1 of Section 3.1 and bulleted items. In the list of threats there is no mention that a card of a specific sensitivity level might be used to access information of that same sensitivity level to which the card processor may not have a need-to-know.
PART 2: PIV-II Section 3.3	Page 12, paragraph 1 of Section 3.3, first bulleted item: "PIV Front-End Subsystem." The implications here are that there will be hardware, software and infrastructure (servers, bridges, routers, switches and cabling etc.) to support this. Where does the funding come from to provide the infrastructure?
PART 2: PIV-II Section 4	Page 17, paragraph 2, last sentence. The text reads: "Formats for mandatory biometric information is defined in Section 4.4." Delete "is and insert: "are."
PART 2: PIV-II	Page 19, Figure 4-1. The PIV card design format indicates that some of the Zones are "optional". This would be a mistake. If

Section Reference	Comment
Section 4.1.4	some areas don't apply to a person, they should indicate "N/A" or something similar, but not be left out. Leaving items blank will make it easier for mistakes during the Authentication process. Of particular interest is Zone 13, "Issue Date", which is a key piece of information. A falsified issue date could be a key indicator of problems during authentication, especially if coupled with special card types. Also, the choice of "Arial" as the font type is unfortunate. This is because Arial (Helvetica) is a sans-serif font, and some letters and numbers can be easily confused, such as capital "I" and lower-case "l". In "Arial" these all look identical. Suggest using a font such as "Tahoma" in communications. A person's name might be misread if "Arial" is used. Page 21, Figure 4-3 (back of military card). The card holder's SSN shouldn't be printed, let's just give everybody their identity so it can be truly stolen! They have all their personal information including DOB here. There should be a cross reference number that internally correlates to the SSN.
PART 2: PIV-II Section 4.1.5.2	Page 23, paragraph 1 of Section 4.1.5.2, sentence 3. The text reads: "The host system can therefore dynamically discover the location and file identifiers associated with the Logical Credential data elements, without the need for a priori knowledge of these." Suggest revising the text by correcting: "a priori" to read "a prior".
PART 2: PIV-II Section 4.1.6.1	Page 24, paragraph 2 of Section 4.1.6.1. Suggest adding the following new last sentence to the paragraph: "The card reader shall not retain in any form the PIN or biometric information used to activate the card."
PART 2: PIV-II Section 4.2.2	Page 26, Table 4-4. SHA-1 (& MD-5 as well) should not be used/allowed through 2010. SHA-1 has well known weakness and a different hash algorithm should be encouraged.
PART 2: PIV-II Section 4.3	Page 27, paragraph 2 of Section 4.3, sentence 1. This document offers a choice between implementing "RSA or elliptic curve private key cryptographic operations." Because these two approaches to public/private cryptography are different, this will lead to incompatibilities between PIV cards while still being FIPS 201 compliant. Suggest revising the text to specify one or the other. Page 27, paragraph 4 of Section 4.3, sentence 1. The text reads: "No cryptographic operations are mandated for the contactless interface…" This will lead to contactless PIV cards that are not capable of secure communications with readers or the ability to perform basic secure authentication operations. This sentence

Section Reference	Comment
	should be removed and sections pertaining to the requirements specific to the secure contactless operations need to be included.
PART 2: PIV-II Section 4.4	Page 30, paragraph 2, sentence 2. Text reads: "Finger prints shall be primary biometric utilized in the PIV system…." Suggest revising the text by inserting "the" before "primary." Page 30, paragraph 2, sentence 3. Text reads: "The recognition rates for facial image are…" Suggest revising the text by inserting "a" before "facial image." Page 30, paragraph 6. Text reads: "The biometric data on the PIV card may only be read from an activated card through the contact interface." This one-sentence paragraph should be revised or removed. Suggest revising this text by specifying the data to be transmitted in a secure manner. If a contactless interface cannot meet the standard, then it should not be used.
PART 2: PIV-II Section 4.4.2	Page 31, Section 4.4.2 on Fingerprint Representation, paragraph 2. Suggest revising the text of paragraph 2 to make it clear up front that the AINSI/NIST -ITL- 1-2000 will be used. Then, suggest revising the text to discuss why the various representation standards are in flux.
PART 2: PIV-II Section 5.2.1.2	Page 42, paragraph 1 of Section 5.2.1.2, sentence 1. The text reads: "…..for current employees expect that…." Need to revise sentence by removing "expect" and inserting "except."
PART 2: PIV-II Section 5.2.1.3	Page 42, paragraph 1 of Section 5.2.1.3, sentence 1. Reference is made to "the Office of Management Budget." Revise the text by adding: "and" before "Budget."
PART 2: PIV-II Section 5.2.3.3	Page 45, paragraph 1 of Section 5.2.3.3. Text reads: "CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum." It would seem that there should be some provision for rapid issue or rapid cancellation when security events occur.
PART 2: PIV-II Section 6.1.4	Bottom of page 52, paragraph 1 of Section 6.1.4, sentence 2. Text reads: "The PACS site-specific symmetric key is stored a PIV local authentication key as defined in Section 4.2." Need to insert "in" between "stored" and "a" for the text to read: "…..key stored in a PIV local…"
PART 2:	Page 53, paragraph 2 of Section 6.2. This paragraph implies that

Section Reference	Comment
PIV-II Section 6.2	the PIV card may be used merely for a visual access card, with no need to have implemented an electronic system. Is this correct? Page 54, paragraphs 3 and 4 of Section 6.2. These paragraphs discuss the advantages and disadvantages of contactless versus contact based physical access control environment. Is there a choice of which environment to use?
PART 2: PIV-II Section 6.3 General	Pages 57 and 58, entire Section 6.3. This section contains the potential for some of the biggest problems; not specifically from the technical perspective, but from the human perspective. In order to validate the card it needs to be physically placed in a reader device or to be read via proximity. Most card key applications require that the card be placed in and left in a reader for the duration of a session, therefore providing a method to insure that when the individual leaves with their card, the system is locked. However, this can lead to cards (badges) being left in machines when a person walks away for a break or lunch.
Annex B: Section B.2	Page 65, Table B-2. The table refers to "soft" and "hard" cards. However, these terms are not defined anywhere in the document. Suggest revising the text to define these terms and add the definitions of these terms to the Glossary.
Annex D: General	Recommend that the following be considered as minimum background checks: a. Education validation - All education starting from High School, there should be no time limit on this. b. Residence History - At least a 5 year residence history, preferably 7 to 10. State, county and city. c. Criminal check in all states of residence - 5 to 7 years. d. Employment history validation - 5 to 7 years. e. Credit Check - 7 years is fine – This validates not only credit, but also can provide identity and location information. f. Citizenship validation - Place of birth, and if necessary immigration information (I-9).
Comments on NIST SP 800-73	
General	Serious problems with references made to other sections of the document, including several incorrect references. Find the use of the word "below" in referring to sections several pages ahead in the document to be misleading and confusing. For example, references such as "Section 6.6 below" are made from Section 3.5 on page 20. Section 6.6 does not appear "below" Section 3.5, but

Section Reference	Comment
	appears on page 80, many pages ahead in the document. Need to check the entire document and revise the references. Please see comments for Sections 3.1.2, 3.1.3, 3.2.2, 3.4.2, 3.5 and 3.6.
Section 1 Introduction	Page 9, paragraph 5. For easier readability, suggest using bullets for the document organization outline. Page 9, paragraph 5. Item that pertains to "Section 8, References. Suggest revising this item to read: "Section 8, References, lists the documents on which Special Publication 800-73 (SP800-73) is based."
Section 2.1 Terms	Helpful that this section is at the beginning of the document. Page 10, definition for "Application Session." Phrase at end of the first sentence that reads: "…is selected or the integrated circuit card is reset." Suggest adding the word "when" between "or" and "the" for the phrase to read: "…is selected or when the integrated circuit card is reset." Page 10, definition for "Card Manager." This definition is vague. Suggest revising. Page 10, definition for "Interface Device." Need to define the term "physical layer communication" and add this definition to the glossary. Page 10, definition for "Key Reference." This definition is vague and needs to be revised. Question: Is the key reference only used in a cryptographic protocol and NOT used in an authentication protocol or a signing protocol? Page 11, definition for "Reset." This definition needs to be revised, especially the phrase "…causes the card to delete all current state and reinitialize itself." Should the phrase be written, "all current states," or "all of its current state?" Page 11, definition for "Status Word." For clarity, suggest revising the definition to read: "Two bytes that are returned by the integrated circuit card to indicate the success of the processed command or to indicate any errors encountered during processing." Page 11, definition for "Template," sentence 2. Need to revise to read: "…..collections of data objects pertaining to…." (Add "s" to the word "object".)
Section 2.2	Basically, this is a good acronym list and it is helpful having it early

Section Reference	Comment
Acronyms	in the document. However, the acronym "PIV" appears twice with two different terms: "Integrated Circuit Card for Identification" and "Personal Identity Verification." Need to select a term for this acronym and use it consistently throughout the document.
Section 2.3	Page 12, paragraph 1, last sentence. Text reads: "Sequences of bytes will be enclosed in be enclosed in apostrophes, for example, '2D' and 3F00'. Need to remove the phrase "in be enclosed," for the phrase to read: "…..will be enclosed in apostrophes…"
Section 3	Page 13, paragraphs 1-4. These paragraphs provide a clear, concise high-level explanation of "concepts and constructs." A basic flow diagram would be helpful. Page 13, paragraph 4, sentence 2. For improved clarity, suggest revising this sentence to read: "Because of this difference, the representation of the PIV concepts and constructs as bits and bytes on the client-application program interface may be different from the representation of these same concepts and constructed on the card command interface." (Place a comma between "difference" and "the" and remove the word "is" from between "interface" and "may."
Section 3.1.2	Page 14, general comment about Section 3.1.2. A basic flow diagram would be helpful in illustrating and clarifying the concept of "data element organization." Page 14, paragraph 7 of Section 3.1.2, sentence 1. The reference "(see 3.5 below)" is incorrect and is a poor reference. The correct section is Section 3.4 and "below" is not the proper reference for a section that appears several pages ahead in the document. Need to revise this reference to state: "(see Section 3.4 of this document)."
Section 3.1.3	Page 15, paragraph 1 of Section 3.1.3, sentence 1. Need to revise sentence to read: "….called the *currently selected dedicated file*." (Add "d" to the word "dedicate.") Page 15, paragraph 2 of Section 3.1.3, sentence 1. Need to remove the reference "(see below)," that does not point to anything.
Section 3.1.4	Page 15, paragraph 2 of Section 3.1.4, sentence 1. Need to revise to read: "…..place the new data element into the proper place within the hierarchy." (Replace "in" with "into" between "element" and "the" and replace "it" with "within" between "place" and "the.")
Section 3.2.2	Bottom of page 16 and up to middle of page 16, paragraph 6 of Section 3.2.2 at the middle of page 16, sentence 1. Revise the end

Section Reference	Comment
	of the sentence to read: "…Section 7 of this document." "Below" is a poor and misleading reference to a section, within the document, that appears several pages ahead.
Section 3.3.2	Page 18, paragraph 5 of Section 3.3.2, sentence 1. Revise this sentence to read: "…security status indicator if it is reset when the currently selected application changes…." (Add the work "when" between "reset" and "the.") Page 18, paragraph 5 of Section 3.3.2, sentence 2. For consistency, suggest revising the end of the sentence to read: "…security status indicator," instead of "…security indicator status."
Section 3.3.3	Bottom of page 18 and top of page 19, paragraph 3 of Section 3.3.3, last sentence that reads: "If the current security status does not indicate that one or the other of these is currently authenticated then the data element could not be read." Find this sentence to be vague and suggest re-writing it.
Section 3.4	Page 19, paragraph 1, sentence 1. Need a reference to Table 3-1 and suggest revising this sentence to read: "…..and described in Table 3-1 that follows." (Remove the phrase "following table" and replace with "Table 3-1 that follows.") Page 19, Table 3-1. All sentence and phrases within the "Comment" column, except for the last phrase, require a "period" at the end. Page 19, Table 3-1, third item in the ""Comment" column. Remove the unnecessary phrase "in which case" from the end of the sentence and place a "period" after the word "object."
Section 3.4.1	Page 19, paragraph 1 of Section 3.4.1, sentence 1. Need to replace "connetion" with "connection."
Section 3.4.2	Page 20, paragraph 2 of Section 3.4.2, last sentence. Need to revise this sentence to read: "The transparent files and dedicated files found in this ADF are described in Section 6.6 of this document." (Add "d" to the word "dedicate" and replace "below" with "of this document." Section 6.6 is several pages ahead in the document and not immediately "below" the paragraph from which this reference is made.)
Section 3.5	Page 20, paragraph 2 of Section 3.5, last sentence. Replace "…Section 6.5 below" with "Section 6.5 of this document," for the same reason as stated in the comment for Section 3.4.2. Page 20, paragraph 3 of Section 3.5, last sentence. Replace "…Section 6.7 below" with "Section 6.7 of this document," for the

Section Reference	Comment
	same reason as stated in the comment for Section 3.4.2. (The correct reference is "Section 6.7" instead of "Section 6.6.") Page 20, paragraph 4 of Section 3.5, sentence 1. Text reads: "Depending on the functionality of an individual card command it may support one or the other or both or neither of these special processing behaviors." This sentence is vague. Suggest revising or removing.
Section 3.6	Bottom of page 20 and top of page 21. Both paragraph 1 and paragraph 2 of this section are vague and need to be revised. Paragraph 1 has a blank (xxx) FIPS reference. A table or diagram would be helpful.